Module 11

Configuring Domain Name System

Contents:

Lesson 1: Install and Configure DNS in an AD DS Domain **11-3**

Lab A: Install the DNS Service **11-11**

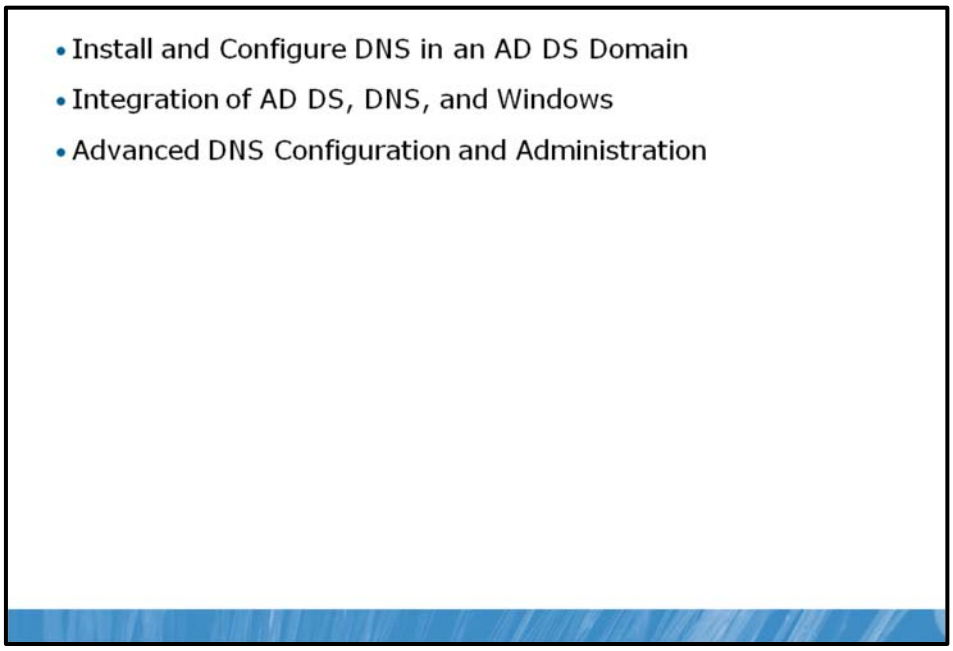
Lesson 2: Integration of AD DS, DNS, and Windows **11-14**

Lesson 3: Advanced DNS Configuration and Administration **11-32**

Lab B: Advanced Configuration of DNS **11-42**

MCT USE ONLY. STUDENT USE PROHIBITED

Module Overview


• Install and Configure DNS in an AD DS Domain
• Integration of AD DS, DNS, and Windows
• Advanced DNS Configuration and Administration

Windows® and Active Directory® services have a strong dependency on Domain Name System (DNS). You will be already familiar with DNS as a user of DNS and as an IT professional supporting users, applications, services, and systems that rely on DNS. In this module, you will learn how to implement DNS to support name resolution both within your Active Directory Domain Services (AD DS) domain, outside your domain, and your intranet.

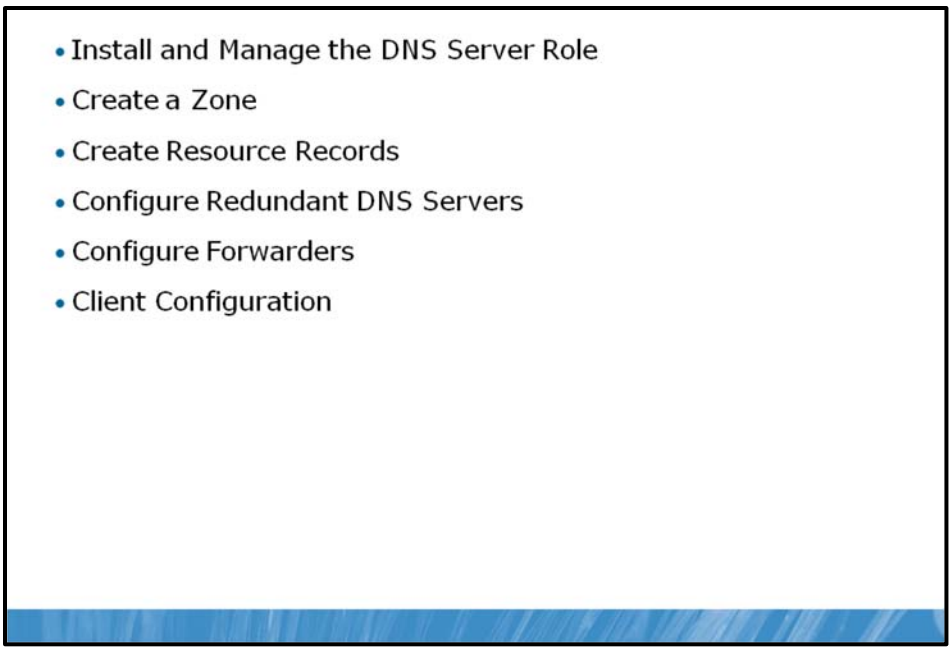
Objectives

After completing this module, you will be able to:

- Describe the concepts, components, and processes of DNS.
- Install and configure DNS.
- Describe how AD DS, DNS, and Windows are integrated.
- Describe the advanced configuration and administration tasks of DNS.

MCT USE ONLY. STUDENT USE PROHIBITED

Lesson 1
Install and Configure DNS in an AD DS Domain



Now that you have reviewed the concepts, terminology, and processes related to DNS and name resolution, you are ready to install and configure the DNS server role in an AD DS domain.

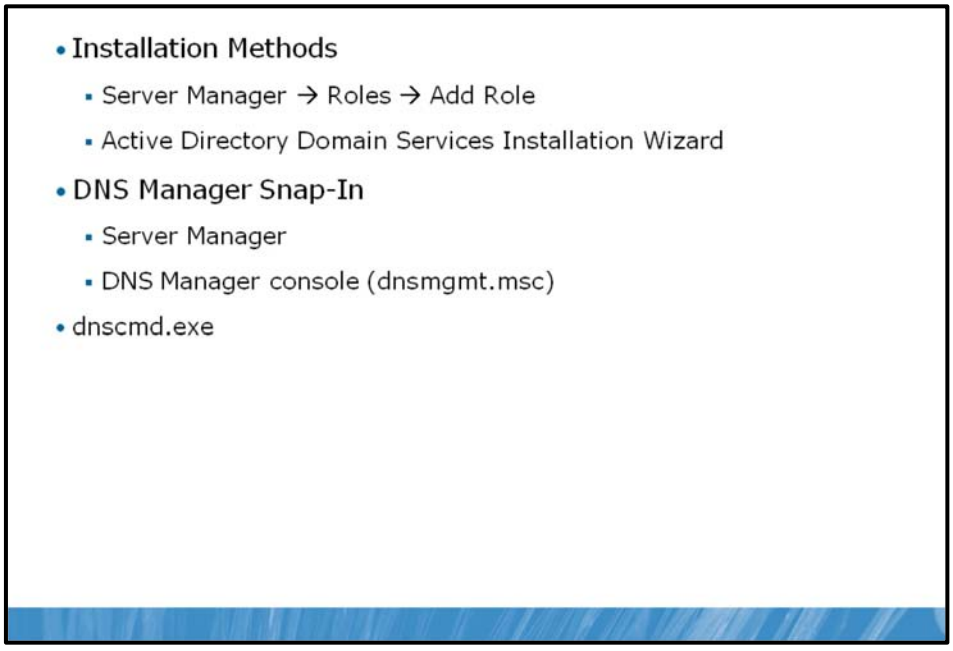
Objectives

After completing this lesson, you will be able to:

- Install DNS.
- Add DNS zones.
- Manage DNS records.
- Configure DNS server settings.
- Configure DNS client settings.

MCT USE ONLY. STUDENT USE PROHIBITED

Install and Manage the DNS Server Role


• Installation Methods
▪ Server Manager → Roles → Add Role
▪ Active Directory Domain Services Installation Wizard
• DNS Manager Snap-In
▪ Server Manager
▪ DNS Manager console (dnsmgmt.msc)
• dnscmd.exe

The DNS server role is not installed on Windows Server® 2008 by default. Like any other functionality, it is added in a role-based manner when a server is configured to perform the role.

You can install the DNS server role by using the Add Role link in Server Manager.

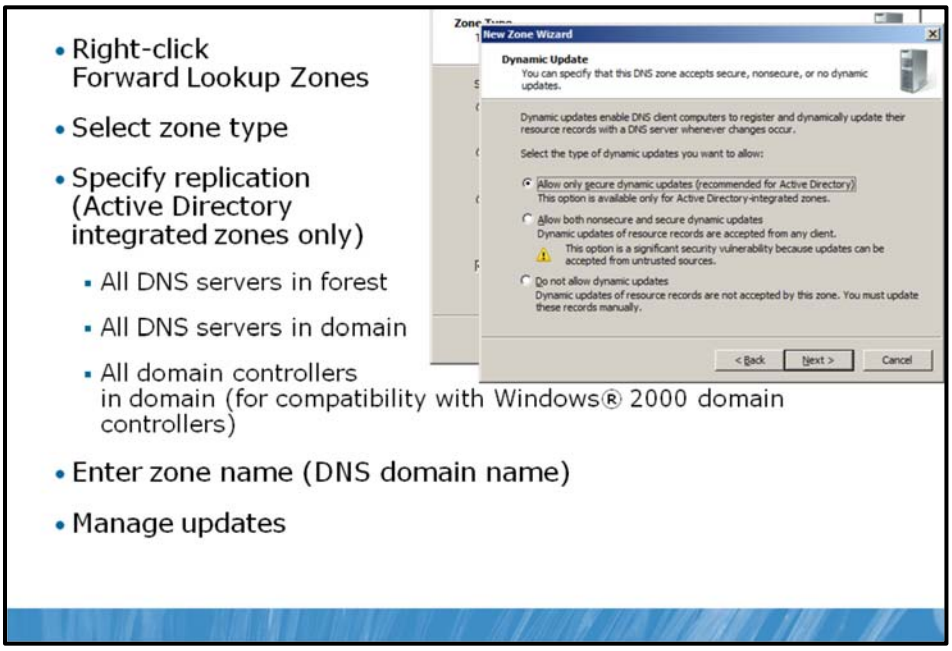
The DNS server role can also be added automatically by the Active Directory Domain Services Installation Wizard, which you can start by using dcpromo.exe. The domain controller options page of the wizard allows you to add the DNS server role.

When the DNS server role is installed, you will find that the DNS Manager snap-in is available to add to your administrative consoles. The snap-in is also added automatically to the Server Manager console and in the DNS Manager console (dnsmgmt.msc). To administer a remote DNS server, add the Remote Server Administrative tools to your administrative workstation that runs Windows Vista® SP1 or later operating systems.

When you install the DNS server role, the dnscmd.exe command-line administrative tool is also added. DNSCmd can be used to script and automate DNS configuration. At the command prompt, type dnscmd.exe /? for help.

MCT USE ONLY. STUDENT USE PROHIBITED

Create a Zone


Right-click Forward Lookup Zones
Select zone type
Specify replication (Active Directory integrated zones only)
All DNS servers in forest
All DNS servers in domain
All domain controllers in domain (for compatibility with Windows® 2000 domain controllers)
Enter zone name (DNS domain name)
Manage updates
New Zone Wizard
Dynamic Update
You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.
Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.
Select the type of dynamic updates you want to allow:
Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.
Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
This option is a significant security vulnerability because updates can be accepted from untrusted sources.
Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.
< Back
Next >
Cancel

After installing a DNS server, you can begin adding zones to the server.

To create a zone, right-click the Forward Lookup Zones node in the console tree and click New Zone. The New Zone Wizard takes you through the process of creating a zone.

You will be able to select one of the three types of zones:

- Primary zone. The DNS server will be able to write to the zone.
- Secondary zone. The DNS server will maintain a copy of a zone hosted on another DNS server. The secondary zone is read-only.
- Stub zone. The DNS server will maintain a list of name servers for another domain. Stub zones will be discussed in detail later in this module.

You can also select to store the zone data in Active Directory if the DNS server is a domain controller. This creates an Active Directory integrated zone, which will be discussed later in this module. If you clear this option, the zone data is stored in a file rather than in Active Directory.

After choosing the zone type, you are prompted to enter the zone name—the fully qualified domain name for the zone.

Zone Updates

When you create a zone, you are also prompted to specify whether dynamic updates are supported. Dynamic updates reduce the management overhead of a zone, because clients can add, delete, and update their own resource records.

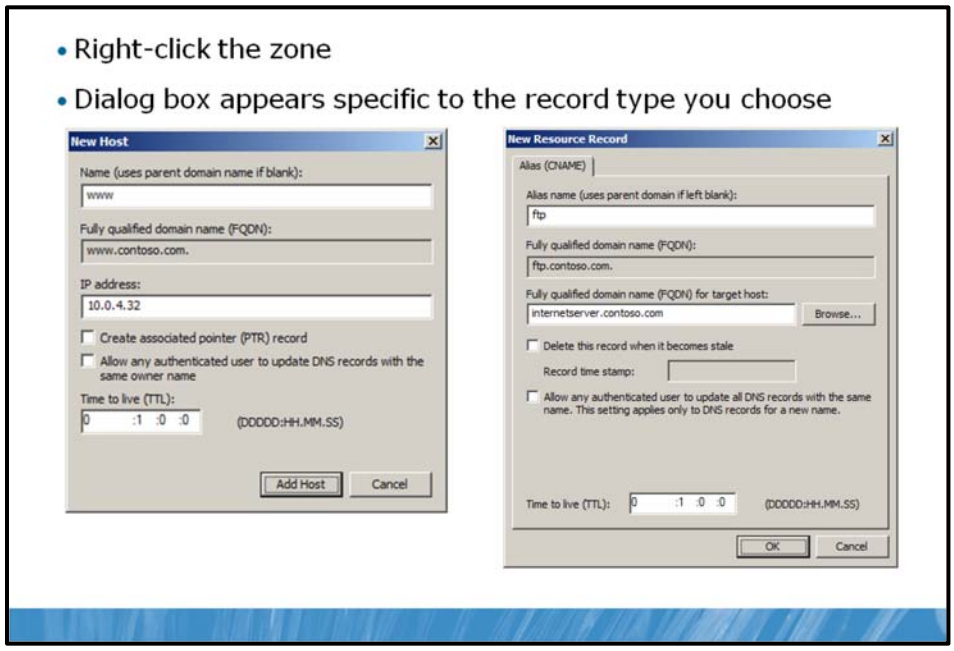
Dynamic updates leave open the possibility that a resource record could be spoofed. For example, a computer could register a record named www, effectively redirecting traffic from your web server to the incorrect address.

MCT USE ONLY. STUDENT USE PROHIBITED

To eliminate the possibility of spoofing, Windows Server 2008 DNS Server service supports secure dynamic updates. A client must authenticate prior to updating its resource records, so the DNS server knows whether the client is the same computer that has the permission to modify the resource record.

MCT USE ONLY. STUDENT USE PROHIBITED

Create Resource Records

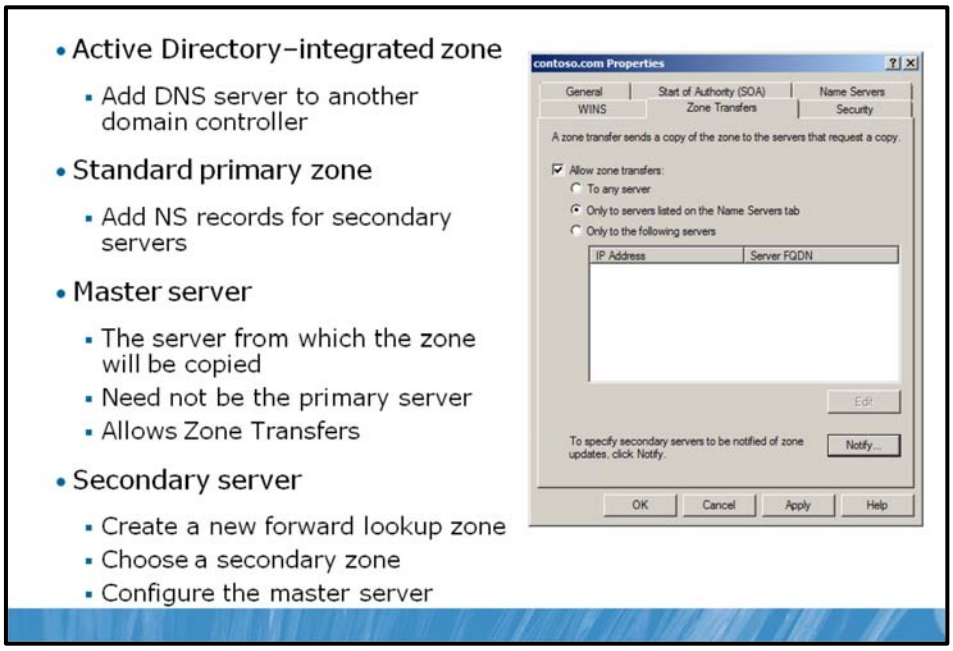

• Right-click the zone
• Dialog box appears specific to the record type you choose
New Host
Name (uses parent domain name if blank):
www
Fully qualified domain name (FQDN):
www.contoso.com.
IP address:
10.0.4.32
Create associated pointer (PTR) record
Allow any authenticated user to update DNS records with the same owner name
Time to live (TTL):
0 :1 :0 :0
(DDDDD:HH.MM.SS)
Add Host
Cancel
New Resource Record
Alias (CNAME)
Alias name (uses parent domain if left blank):
ftp
Fully qualified domain name (FQDN):
ftp.contoso.com.
Fully qualified domain name (FQDN) for target host:
internetserver.contoso.com
Browse...
Delete this record when it becomes stale
Record time stamp:
Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.
Time to live (TTL):
0 :1 :0 :0
(DDDDD:HH.MM.SS)
OK
Cancel

In most environments, even those with dynamic updates enabled, there will be the need to add resource records to a zone.

To create a resource record, right-click the zone and choose the type of record you wish to create. A dialog box appears with input controls that are appropriate for the type of record you are adding. Besides entering a resource record name and an IP address, you can manually set the TTL period, and you can configure options for updating records and pointer records.

MCT USE ONLY. STUDENT USE PROHIBITED

Configure Redundant DNS Servers


• Active Directory–integrated zone
▪ Add DNS server to another domain controller
• Standard primary zone
▪ Add NS records for secondary servers
• Master server
▪ The server from which the zone will be copied
▪ Need not be the primary server
▪ Allows Zone Transfers
• Secondary server
▪ Create a new forward lookup zone
▪ Choose a secondary zone
▪ Configure the master server
contoso.com Properties
General
Start of Authority (SOA)
Name Servers
WINS
Zone Transfers
Security
A zone transfer sends a copy of the zone to the servers that request a copy.
Allow zone transfers:
To any server
Only to servers listed on the Name Servers tab
Only to the following servers
IP Address
Server FQDN
Edit...
To specify secondary servers to be notified of zone updates, click Notify.
Notify...
OK
Cancel
Apply
Help

An enterprise should strive to ensure that a zone can be resolved authoritatively by at least two DNS servers.

If the zone is Active Directory–integrated, you can simply add the DNS server role to another domain controller in the same domain as the first DNS server. Active Directory–integrated zones and the replication of the DNS zone by AD DS are described in the next lesson.

If the zone is not Active Directory-integrated, you must add another DNS server and configure it to host a secondary zone. Remember that a secondary zone is a read-only copy of the primary zone. A secondary zone can be used for name resolution, but not for records management. All changes are pulled from the primary zone.

The first step in this process is to configure the zone itself to refer to the secondary servers as name servers for the zone. Then, add naming service records for the secondary servers to the parent zone.

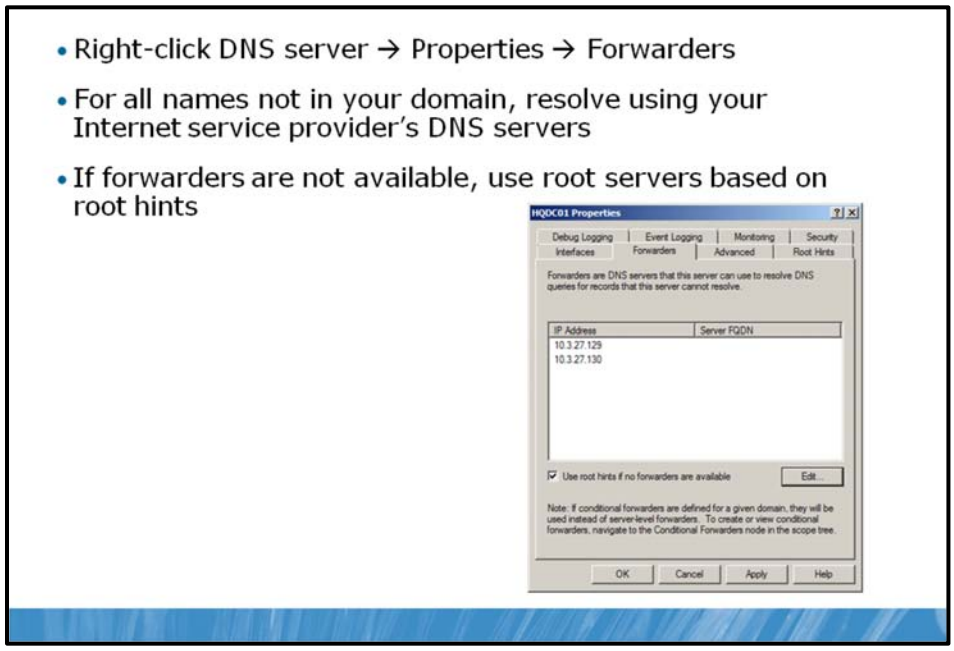
A secondary server copies the zone from another DNS server called the master server. The master server need not be the primary server, but there are obvious advantages to using the primary zone as the master to reduce the latency with which record updates are replicated to secondary servers.

The master server must allow the secondary servers to connect and initiate a zone transfer. This is configured on the Zone Transfers tab of the zone properties on the master server, shown on the slide:

You can then add the secondary zone to the forward lookup zones of the secondary server. The secondary server is configured to replicate the zone from the master server.

MCT USE ONLY. STUDENT USE PROHIBITED

Configure Forwarders


• Right-click DNS server → Properties → Forwarders
• For all names not in your domain, resolve using your Internet service provider's DNS servers
• If forwarders are not available, use root servers based on root hints
HQDC01 Properties
Debug Logging
Event Logging
Monitoring
Security
Interfaces
Forwarders
Advanced
Root Hints
Forwarders are DNS servers that this server can use to resolve DNS queries for records that this server cannot resolve.
IP Address
Server FQDN
10.3.27.129
10.3.27.130
Use root hints if no forwarders are available
Edit...
Note: If conditional forwarders are defined for a given domain, they will be used instead of server-level forwarders. To create or view conditional forwarders, navigate to the Conditional Forwarders node in the scope tree.
OK
Cancel
Apply
Help

In Lesson 1, you learned that a DNS server attempts to resolve a client's query by using its local zones and cache. If it is unable to do so, and if the query is sent as a recursive query, the DNS server performs the query on behalf of the client.

To configure a DNS server to effectively perform a recursive query, the first method is to add forwarders to the DNS server. Forwarders are pointers to other DNS servers. Typically, these servers are hosted by your Internet service provider (ISP), or they are configured as upstream DNS servers in your enterprise DNS infrastructure. For example, your Active Directory domain may use Windows DNS Server service to resolve names within the domain, and then forward queries to your corporate DNS servers, which host zones for other enterprise domains.

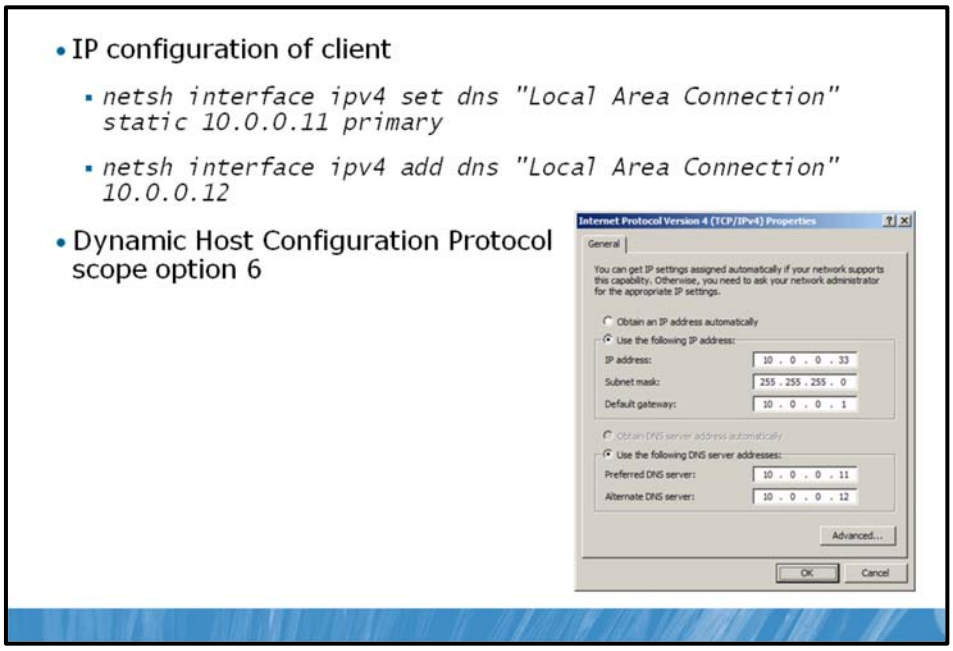
Forwarders are similar to the DNS servers that you configure in the IP properties of a network connection. That list of DNS servers is used by the DNS Client service. The list is not shared with the DNS server service. Forwarders serve the same purpose for the DNS server service.

If forwarders are not configured, the server will attempt to query a name server for the root of the DNS namespace ("."). These root servers are maintained as root hints. Although the root DNS name servers do not change frequently, they can change occasionally. Windows Update will include updates to the root hints.

There are several mechanisms with which a recursive query can be made more efficient, including conditional forwarders and stub zones. These options will be discussed in Lesson 4.

MCT USE ONLY. STUDENT USE PROHIBITED

Client Configuration


• IP configuration of client
▪ netsh interface ipv4 set dns "Local Area Connection" static 10.0.0.11 primary
▪ netsh interface ipv4 add dns "Local Area Connection" 10.0.0.12
• Dynamic Host Configuration Protocol scope option 6
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 10 . 0 . 0 . 33
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 10 . 0 . 0 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 10 . 0 . 0 . 11
Alternate DNS server: 10 . 0 . 0 . 12
Advanced...
OK
Cancel

A DNS server is not of much use unless clients are configured to query it. The DNS client is distinct from all Active Directory–related components of the Windows operating system. Therefore, a client does not assume that its domain controller is a DNS server. A client should have at least two DNS servers configured.

The configuration can be fixed in the client's IP configuration, as shown in the screen shot:

The netsh.exe command can also be used to configure the first and additional DNS servers for a network connection, as in the following example:

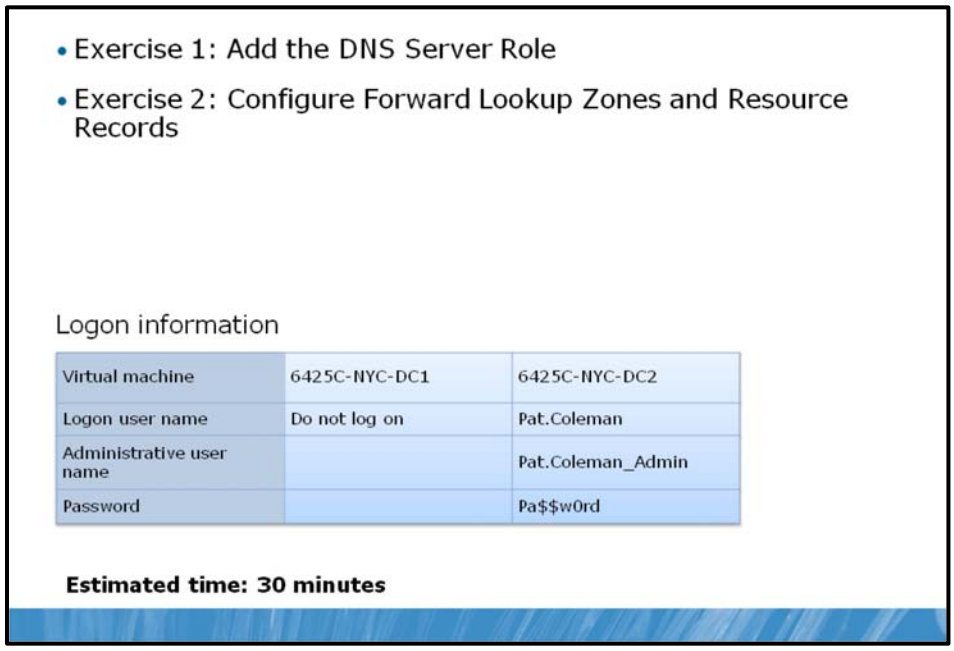
```
netsh interface ipv4 set dns "Local Area Connection"
static 10.0.0.11 primary
netsh interface ipv4 add dns "Local Area Connection"10.0.0.12
```

Alternatively, the DNS servers can be passed to clients through Dynamic Host Configuration Protocol (DHCP) by using the DHCP scope option 6: DNS server.

Remember that secondary and additional DNS servers are not queried if the primary DNS server returns a negative response. Additional DNS servers are queried only if the primary DNS server does not respond, and is offline.

MCT USE ONLY. STUDENT USE PROHIBITED

Lab A: Install the DNS Service


• Exercise 1: Add the DNS Server Role
• Exercise 2: Configure Forward Lookup Zones and Resource Records
Logon information
Virtual machine | 6425C-NYC-DC1 | 6425C-NYC-DC2
Logon user name | Do not log on | Pat.Coleman
Administrative user name | | Pat.Coleman_Admin
Password | | Pa$$w0rd
Estimated time: 30 minutes

Lab Setup

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Hyper-V™ Manager, click **6425C-NYC-DC1**, and in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts. Do not log on to NYC-DC1 until directed to do so.
4. Repeat steps 2 and 3 for **6425C-NYC-DC2.**
5. Log on to NYC-DC2 by using the following credentials:
   - User name: **Pat.Coleman**
   - Password: **Pa$$w0rd**
   - Domain: **Contoso**

Lab Scenario

You are an administrator at Contoso, Ltd. You recently added a second domain controller to your enterprise, and you want to add redundancy to the DNS server hosting the domain's zone. Currently, the only DNS server for the contoso.com zone is NYC-DC1. You need to ensure that clients that resolve against the new DNS server, NYC-DC2, can access Internet websites. Additionally, you need to configure a subdomain to support name resolution required for the testing of an application by the development team.

MCT USE ONLY. STUDENT USE PROHIBITED

MCT USE ONLY. STUDENT USE PROHIBITED

Exercise 1: Add the DNS Server Role

In this exercise, you will add the DNS server role to NYC-DC2, examine the domain zone that is automatically populated on the DNS server, and then configure NYC-DC2 to use itself as its primary DNS server.

1. Add the DNS server role.
2. Change the DNS server configuration of the DNS client.
3. Examine the domain forward lookup zone.
4. Configure forwarders for Internet name resolution.

▶ Task 1: Add the DNS server role.

1. On NYC-DC2, run Server Manager as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa$$w0rd**.
2. Add the DNS server role to NYC-DC2.
3. Close Server Manager.
4. Restart NYC-DC2. Then log on as **Pat.Coleman** with the password **Pa$$w0rd**.

   This is not necessary in a production environment, but it speeds up the process of restarting services and replicating the DNS records to NYC-DC2 for the purposes of this exercise.

▶ Task 2: Change the DNS server configuration of the DNS client.

1. Log on to NYC-DC2 as **Pat.Coleman** with the password **Pa$$w0rd.**
2. Run the command prompt as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa$$w0rd**.
3. Type **netsh interface ipv4 set dnsservers "Local Area Connection" static 10.0.0.11 primary** and then press Enter.
4. Type **netsh interface ipv4 add dnsservers "Local Area Connection" 10.0.0.10** and then press Enter.

▶ Task 3: Examine the domain forward lookup zone.

1. Run DNS Manager as an administrator on NYC-DC1, with the user name **Pat.Coleman_Admin** and the password **Pa$$w0rd**.
2. Examine the SOA, NS, and A records in the contoso.com forward lookup zone.

▶ Task 4: Configure forwarders for Internet name resolution.

- Configure two forwarders for NYC-DC2**:** 192.168.200.12 and 192.168.200.13. Because these DNS servers do not actually exist, the Server FQDN will display either <Attempting to resolve> or <Unable to resolve>. In a production environment, you would configure forwarders to upstream DNS servers on the Internet; usually those provided by your ISP.

Results: In this exercise, you added the DNS server role to NYC-DC2 and simulated the configuration of forwarders to resolve Internet DNS names.

Exercise 2: Configure Forward Lookup Zones and Resource Records

In this exercise, you will add a forward lookup zone for the development domain at Contoso, Ltd. You will then add a host and CNAME record to the zone and confirm that name resolution for the new zone is functioning.

The main tasks for this exercise are as follows:

1. Create a forward lookup zone.
2. Create Host and CNAME records.
3. Test name resolution.

▶ Task 1: Create a forward lookup zone.

- Create a new forward lookup zone named **development.contoso.com**. The zone should be a primary zone, stored in Active Directory and replicated to all domain controllers in the contoso.com domain. Configure the zone so that it does not allow dynamic updates.

Note In a production environment, you would most likely just replicate to all DNS servers. However, for this lab, you will replicate to all domain controllers to ensure quick and guaranteed replication.

▶ Task 2: Create Host and CNAME records.

1. In the development.contoso.com zone, create a host (A) record for APPDEV01 with the IP address **10.0.0.24**.
2. Create a CNAME record, **www.development.contoso.com** that resolves to **appdev01.development.contoso.com**.

▶ Task 3: Test name resolution.

- At the command prompt, type **nslookup www.development.contoso.com**, and then press Enter.

  Examine the output of the command. What does the output tell you?

Results: In this exercise, you created a new forward lookup zone, development.contoso.com, with host and CNAME records, and verified that names in the zone can be resolved.

Note Do not shut down the virtual machines after you finish this lab because the settings you have configured here will be used in the next lab.

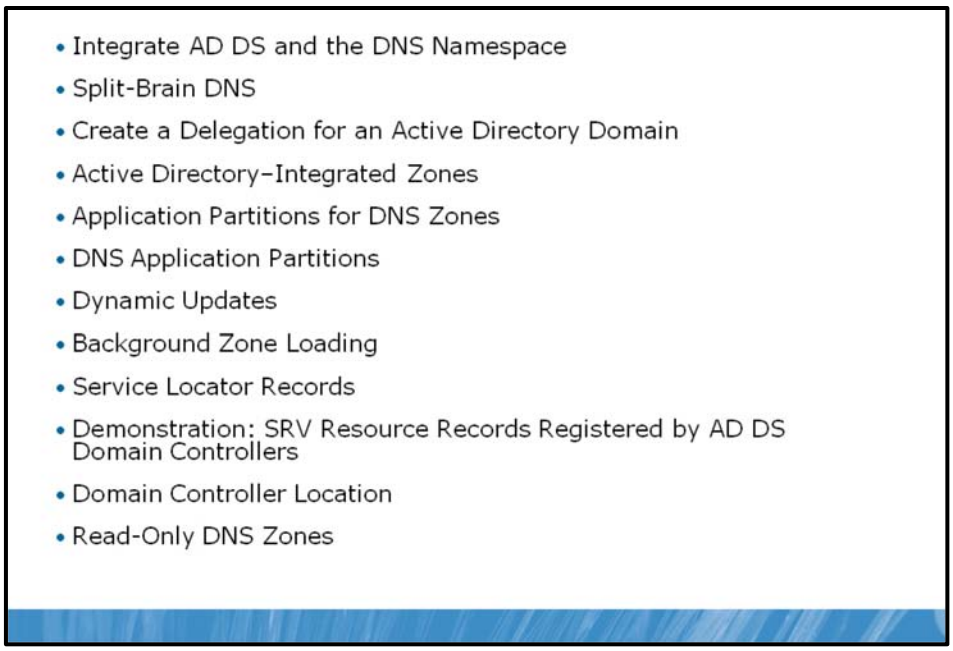
Lab Review Questions

Question: If you did not configure forwarders on NYC-DC2, what would be the result for clients that use NYC-DC2 as their primary DNS server?

Question: What would happen to clients' ability to resolve names in the development.contoso.com domain if you had chosen a stand-alone DNS zone, rather than an Active Directory–integrated zone? Why would this happen? What should you do to solve this problem?

MCT USE ONLY. STUDENT USE PROHIBITED

Lesson 2
Integration of AD DS, DNS, and Windows


• Integrate AD DS and the DNS Namespace
• Split-Brain DNS
• Create a Delegation for an Active Directory Domain
• Active Directory–Integrated Zones
• Application Partitions for DNS Zones
• DNS Application Partitions
• Dynamic Updates
• Background Zone Loading
• Service Locator Records
• Demonstration: SRV Resource Records Registered by AD DS Domain Controllers
• Domain Controller Location
• Read-Only DNS Zones

You've learned to configure DNS in a simple environment by using many of the default settings that support Active Directory domains out of the box. In this lesson, you will learn more about the components and processes that support AD DS and the interrelation between AD DS and DNS.

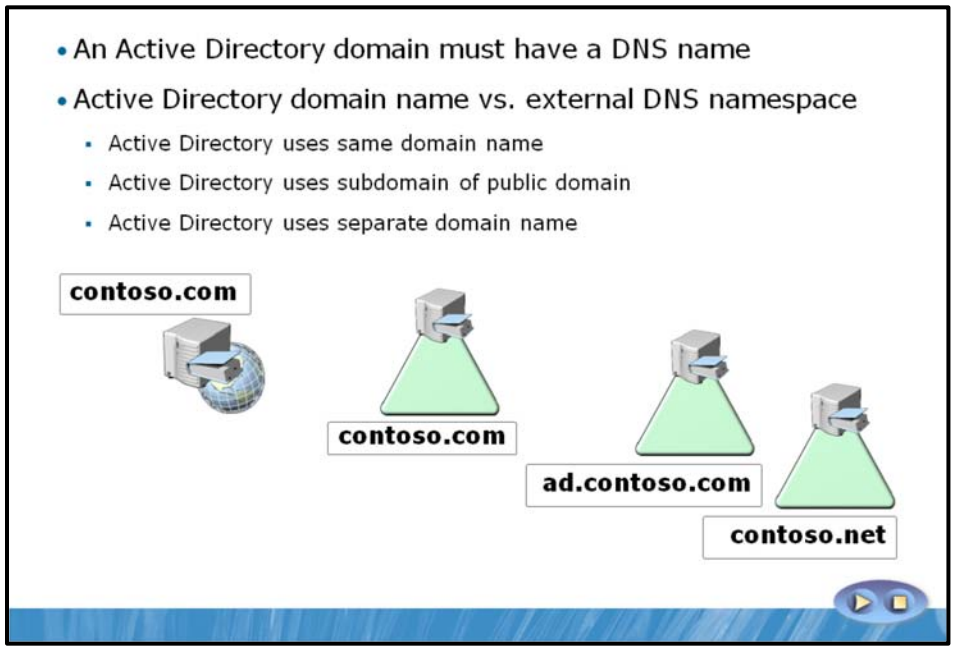
Objectives

After completing this lesson, you will be able to:

- Understand the integration between AD DS and DNS.
- Choose a DNS domain for an Active Directory domain.
- Create a zone delegation for a new Active Directory domain.
- Configure replication for Active Directory-integrated zones.
- Describe the purpose of SRV records in the domain controller location process.
- Understand read-only DNS servers.

MCT USE ONLY. STUDENT USE PROHIBITED

Integrate AD DS and the DNS Namespace


An Active Directory domain must have a DNS name
Active Directory domain name vs. external DNS namespace
Active Directory uses same domain name
Active Directory uses subdomain of public domain
Active Directory uses separate domain name
contoso.com
contoso.com
ad.contoso.com
contoso.net

Active Directory requires DNS, and an AD DS domain must have a DNS domain name. Because DNS is also used as a globally available, standards-based namespace, you should carefully consider where in the namespace you set your AD DS domain.

Let's assume that you are an administrator of Contoso, Ltd, which maintains the registered domain name contoso.com, and which has a website at www.contoso.com. If you are planning the namespace for your AD DS domain, you could choose one of the following:

- The same domain name as your external DNS domain name: contoso.com. If you use the same namespace, you have to implement split-brain DNS, which is described in the next section.
- A subdomain of your external domain name: ad.contoso.com. If you use a subdomain of a registered domain name, you can proceed easily because you are the owner of that portion of the DNS namespace. You should be careful, however, of going too deep in the DNS namespace. Users and admins alike will be typing fully qualified domain names frequently, and a lengthy domain suffix will make each FQDN more difficult to enter. In addition, URLs and UNCs have length limits, which are easier to reach with lengthy DNS suffixes.
- A separate domain name: contoso.net. If you use a separate domain name for your Active Directory domain, register the domain so that it is not usurped by another organization. Ensure that you maintain ownership of that portion of the DNS namespace.

In today's increasingly connected world, the lines between network, intranet, extranet, and the Internet are blurred. It is becoming difficult to maintain namespace separation and less value is contributed by it. For this reason, many organizations are choosing to use the most familiar domain name: the public domain name. The public domain name is the one most closely associated with the organization and the domain name that's easiest to type. As already mentioned, there are steps you must take to support this configuration, but the cost of the steps is typically far less than the benefits it provides. With any of these choices, you must manage name resolution, perimeter protection, and security, so there are equivalent

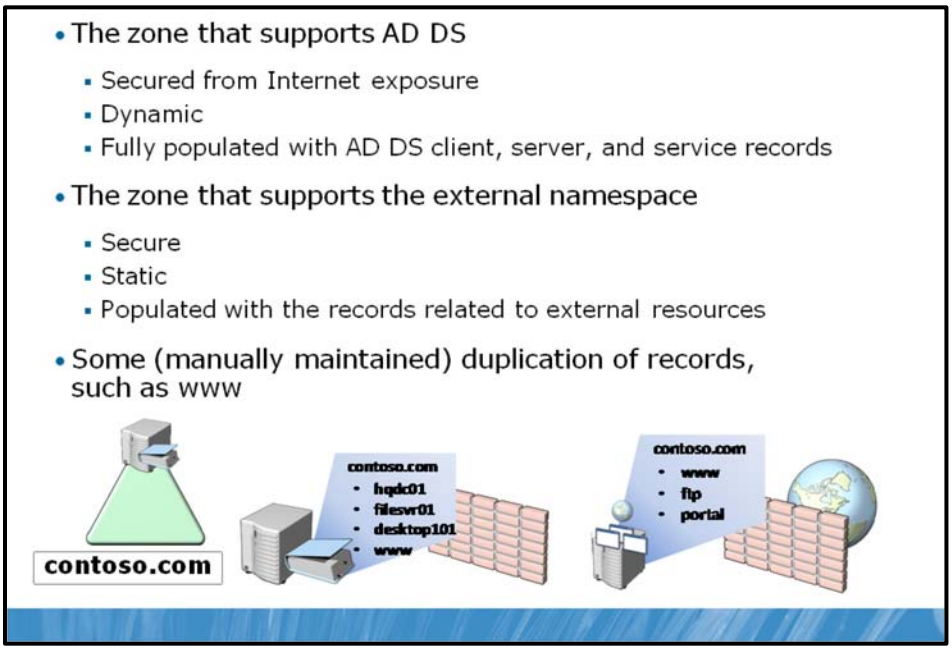
MCT USE ONLY. STUDENT USE PROHIBITED

levels of administrative effort to support any of these namespace choices. Therefore, use a DNS name that is easy for the users of your namespace.

In the early years of Active Directory, it was common to suggest the use of a custom top-level domain, such as .msft or even the .local top-level domain for the Active Directory domain. Due to changes in the networked world, including IP version 6 (IPv6)and increased interconnectivity, these options should be explored only after very careful consideration of their ability to support your business requirements, the benefits they might provide, and the cost in terms of administration and user support.

MCT USE ONLY. STUDENT USE PROHIBITED

Split-Brain DNS



Whenever you use a domain name for an AD DS domain that is also used for connections to your network from the outside world, ensure that there is a separation of DNS zones that provides different information to public and internal clients. This is called split-brain DNS. In fact, you use separate DNS servers to answer queries for the same domain name. Internal DNS answers queries coming only from your local clients, whereas external DNS answers queries only from external clients. No client should be available to access both DNS servers at the same time.

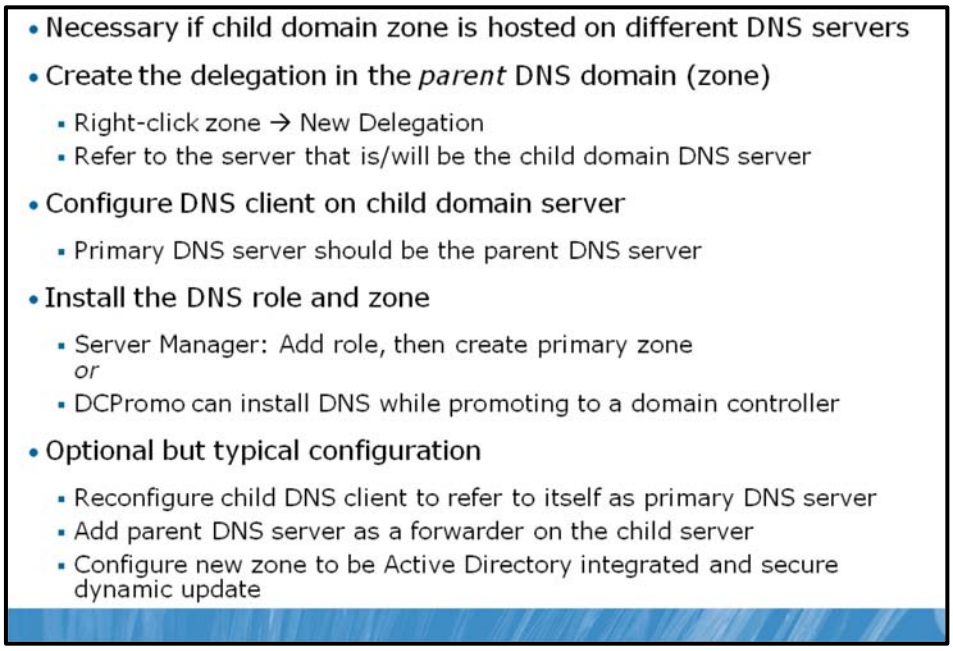
The internal DNS zone must support the AD DS domain in full fidelity, with all of the resource records for servers, clients, and services in the domain. Ideally, it allows secure dynamic updates and stores its zone data in Active Directory itself.

The externally accessible DNS zone provides to outside clients only the resource records that they require, for example, www and ftp. This zone will typically be much smaller than the zone supporting the domain internally. The external zone will typically be updated manually, rather dynamically. The DNS Server hosting the external zone will often be placed behind the external firewall, with only port 53 opened to it.

There may well be some need for duplicate records in the two zones. If your internal users need access to the public website, such as www.contoso.com, that resource record must exist in the internal zone against which clients query. Remember, because the internal DNS server is considered authoritative for the zone (as is the external server), it will return either a resolution for a query or a negative response, indicating that the record simply doesn't exist. There is no "second query" or iterative query against the external zone. Therefore, you will create records that are required internally and externally, such as www, in both zones.

MCT USE ONLY. STUDENT USE PROHIBITED

Create a Delegation for an Active Directory Domain


• Necessary if child domain zone is hosted on different DNS servers
• Create the delegation in the *parent* DNS domain (zone)
▪ Right-click zone → New Delegation
▪ Refer to the server that is/will be the child domain DNS server
• Configure DNS client on child domain server
▪ Primary DNS server should be the parent DNS server
• Install the DNS role and zone
▪ Server Manager: Add role, then create primary zone
or
▪ DCPromo can install DNS while promoting to a domain controller
• Optional but typical configuration
▪ Reconfigure child DNS client to refer to itself as primary DNS server
▪ Add parent DNS server as a forwarder on the child server
▪ Configure new zone to be Active Directory integrated and secure dynamic update

In Module 1, you created a new Windows Server 2008 AD DS domain and forest. When you promoted the domain controller, you received a message indicating that there was no delegation for the contoso.com domain. You ignored the message, and the domain was established with DNS on the domain controller. Clients configured with the IP address of the domain controller as their DNS server will query the DC and can resolve names in the contoso.com domain. However, no external clients can resolve contoso.com names because there is no delegation—no Name Service records in the .com domain that point to your authoritative DNS server.

This is not a problem for the labs in this course because your domain is separated from the rest of the Internet, and there is no need for a delegation.

However, within a forest, it is important that there are delegations from a parent to a child domain if the child domain's zone will be hosted on separate DNS servers. If the child domain is a subdomain of the existing zone, no delegation is necessary.

For example, to add a domain, europe.contoso.com, to the domain tree, and to support replication and authentication in the forest, clients in contoso.com must be able to resolve servers, services, and other records in europe.contoso.com.

Before you add a child domain to a tree, or a new tree to a forest, you must create a delegation in the parent domain or the forest root domain.

To create a delegation, right-click the zone for the parent domain and choose New Delegation. You will be prompted to enter name servers for the new domain. Refer to the server that is or will be the child domain's DNS server.

To create a delegation for a new domain tree or for the forest root domain itself, create a new zone first in the existing root DNS zone. In the new zone, add an Address record that uses the full DNS name of the new domain's DNS server. Then, add an NS record for the new domain that refers to the full DNS name of the domain controller.

MCT USE ONLY. STUDENT USE PROHIBITED

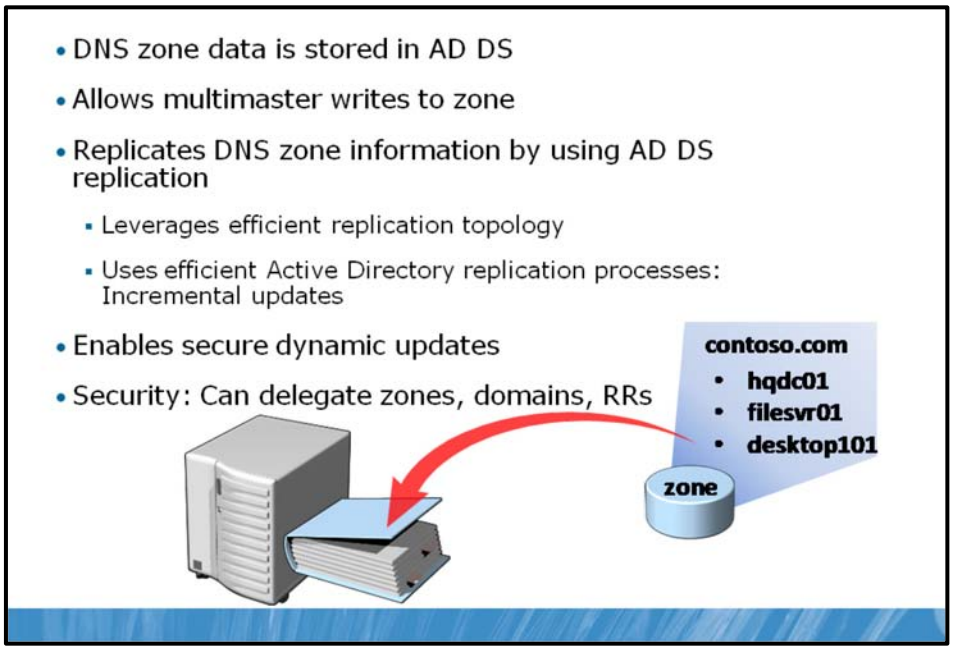
After you've created the delegation, you are ready to configure the server that will be the child domain's first domain controller. First, configure its DNS server to point to the DNS server on which you created the delegation.

Install the DNS role by using Server Manager and then create the primary zone for the child domain. Alternatively, use the Active Directory Domain Services Installation Wizard (dcpromo.exe), which can install DNS as part of the installation of AD DS.

After the child domain has been created, reconfigure the child DNS server to refer to itself as its primary DNS server. Typically, you will add the parent DNS server as a forwarder, conditional forwarder, or stub zone to the child DNS server. You must ensure, one way or another, that systems in the child domain can resolve names in the parent domain. Finally, use an Active Directory–integrated zone that supports secure dynamic updates for the child domain.

MCT USE ONLY. STUDENT USE PROHIBITED

Active Directory–Integrated Zones

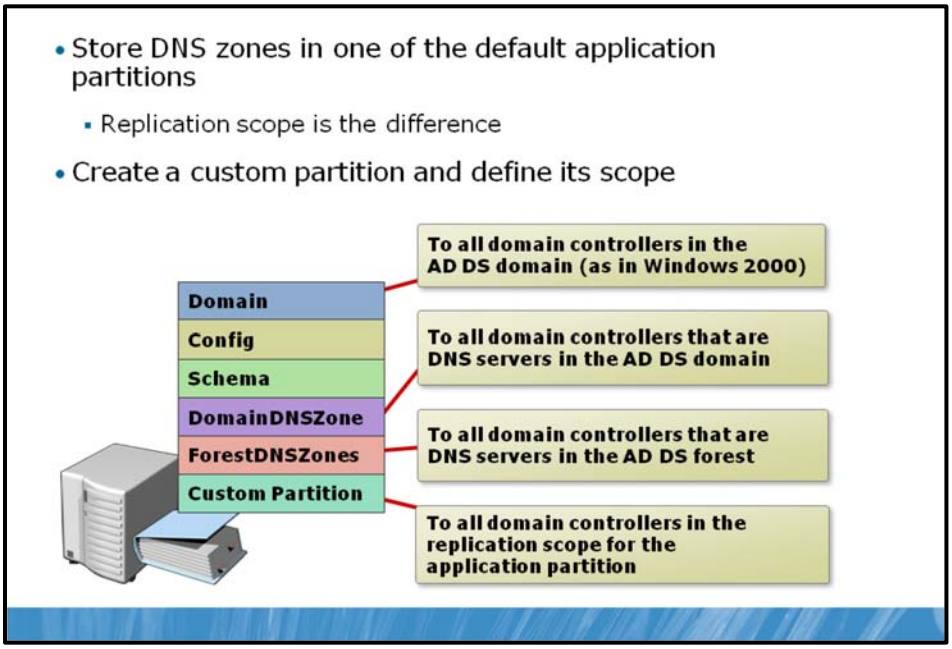

• DNS zone data is stored in AD DS
• Allows multimaster writes to zone
• Replicates DNS zone information by using AD DS replication
▪ Leverages efficient replication topology
▪ Uses efficient Active Directory replication processes: Incremental updates
• Enables secure dynamic updates
• Security: Can delegate zones, domains, RRs
contoso.com
• hqdc01
• filesvr01
• desktop101
zone

In Lesson 1, you learned that Windows DNS Server can store zone data in the AD DS database when the DNS server is an AD DS domain controller. This creates an Active Directory–integrated zone. The benefits of Active Directory–integrated zones are significant:

- Multimaster updates. Unlike standard primary zones, which can only be modified by a single primary server, Active Directory–integrated zones can be written to by any DC to which the zone is replicated. This removes a single point of failure in the DNS infrastructure. It is particularly important in geographically distributed environments that use dynamic update zones, because it allows clients to update their DNS records without having to connect to a potentially distant primary server.
- Replication of DNS zone data by using AD DS replication. In Module 13, you will learn about the efficient topology-generating and replication mechanisms of AD DS replication. One of the characteristics of Active Directory replication is attribute-level replication in which only changed attributes are replicated. An Active Directory–integrated zone can leverage these benefits of Active Directory replication, rather than replicating the entire zone file as in traditional DNS zone transfer models.
- Secure dynamic updates. An Active Directory–integrated zone can enforce secure dynamic updates.
- Granular security. As with other Active Directory objects, an Active Directory-integrated zone allows you to delegate administration of zones, domains, and resource records by modifying the access control list (ACL) on the object.

MCT USE ONLY. STUDENT USE PROHIBITED

Application Partitions for DNS Zones

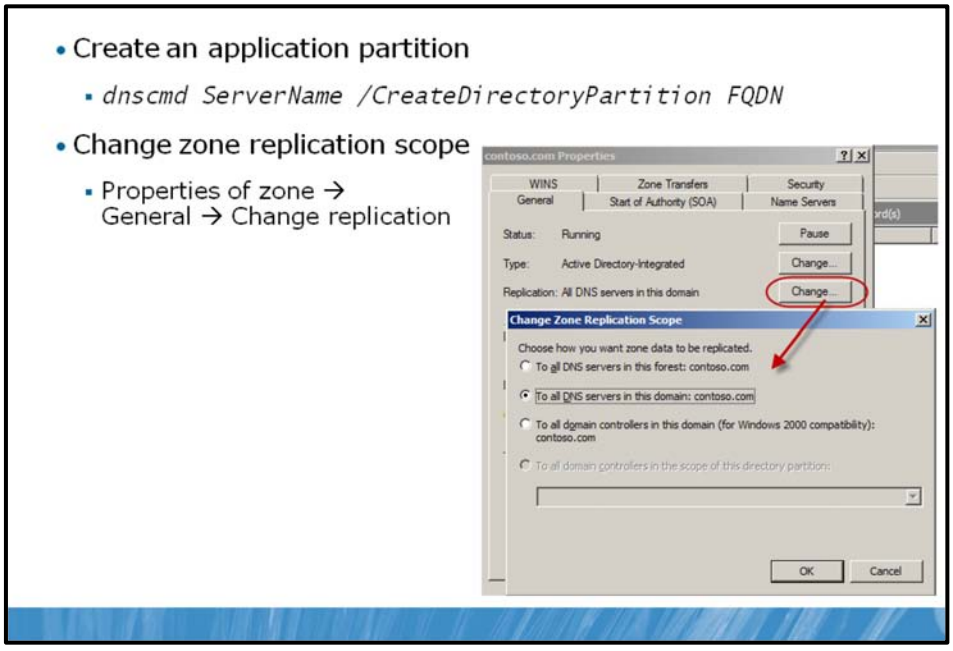

Store DNS zones in one of the default application partitions
Replication scope is the difference
Create a custom partition and define its scope
Domain
Config
Schema
DomainDNSZone
ForestDNSZones
Custom Partition
To all domain controllers in the AD DS domain (as in Windows 2000)
To all domain controllers that are DNS servers in the AD DS domain
To all domain controllers that are DNS servers in the AD DS forest
To all domain controllers in the replication scope for the application partition

An Active Directory integrated zone stores its records in the AD DS database. The records can be stored in one of several partitions:

- DomainDNSZone partition. This partition is replicated to all domain controllers that are DNS servers within the domain.
- ForestDNSZones partition. This partition is replicated to all domain controllers that are DNS servers in the forest.
- These default partitions are created when DNS is installed and configured during AD DS installation. You can use the DNS management tool or the dnscmd.exe command to create the partitions after AD DS is installed.
- Domain partition. This partition, which also contains records for objects, users, and computers, is replicated to all domain controllers, whether or not they are DNS servers. In Windows 2000, DNS zones were stored in the Domain NC. If you have Windows 2000 domain controllers that are DNS servers, use this replication option to support those systems.
    - Your choice of partition is primarily a matter of selecting the replication topology you want for your DNS zones. Of course, the zone must be replicated to a DNS server for that DNS server to be authoritative for the zone. If a DNS server does not have a replica of the zone, it must have a forwarder or stub zone to perform recursive queries for names in the zone.
- Custom application partition. If the default application partitions do not give you the replication model that you require to support your DNS infrastructure, you can create a custom application partition for which you can specify which servers will replicate the partition.

MCT USE ONLY. STUDENT USE PROHIBITED

DNS Application Partitions


• Create an application partition
▪ dnscmd ServerName /CreateDirectoryPartition FQDN
• Change zone replication scope
▪ Properties of zone → General → Change replication
contoso.com Properties
WINS
Zone Transfers
Security
General
Start of Authority (SOA)
Name Servers
Status: Running
Pause
Type: Active Directory-Integrated
Change...
Replication: All DNS servers in this domain
Change...
Change Zone Replication Scope
Choose how you want zone data to be replicated.
To all DNS servers in this forest: contoso.com
To all DNS servers in this domain: contoso.com
To all domain controllers in this domain (for Windows 2000 compatibility): contoso.com
To all domain controllers in the scope of this directory partition:
OK
Cancel

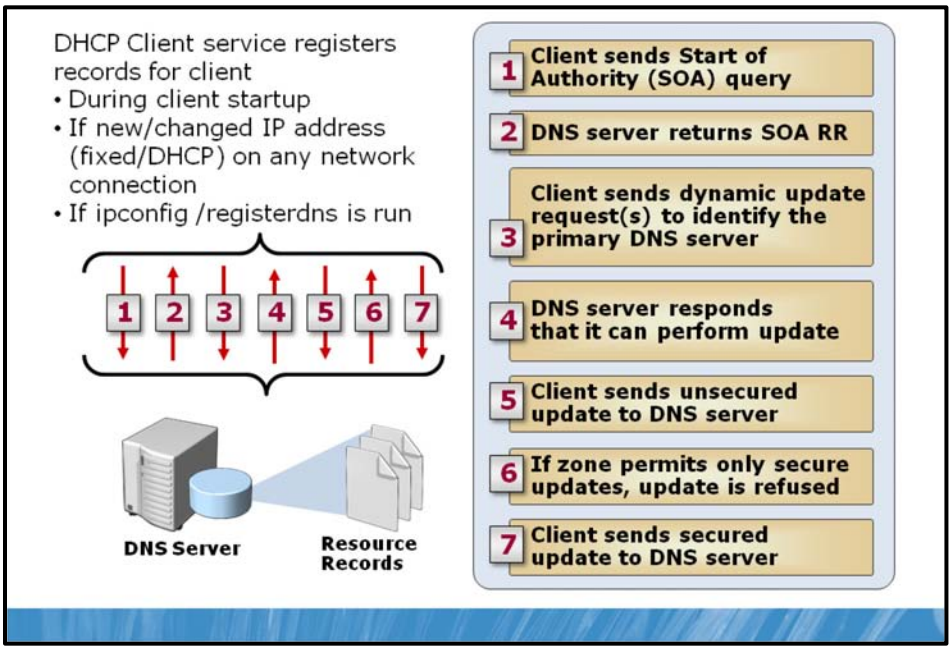
You can create an application partition by using the dnscmd.exe command, as in the following example:

```
dnscmd NYC-DC1.contoso.com /createdirectorypartition MyZone.contoso.com
```

You can change the replication scope of a zone from its properties. Click the Change button next to Replication, as shown in the figure on the slide.

MCT USE ONLY. STUDENT USE PROHIBITED

Dynamic Updates


DHCP Client service registers records for client
• During client startup
• If new/changed IP address (fixed/DHCP) on any network connection
• If ipconfig /registerdns is run
1 2 3 4 5 6 7
DNS Server
Resource Records
1 Client sends Start of Authority (SOA) query
2 DNS server returns SOA RR
3 Client sends dynamic update request(s) to identify the primary DNS server
4 DNS server responds that it can perform update
5 Client sends unsecured update to DNS server
6 If zone permits only secure updates, update is refused
7 Client sends secured update to DNS server

By default, Windows systems attempt to register their records with their DNS server. This behavior can be modified in the IP configuration of the client or through Group Policy.

It is the DHCP Client service that performs the registration, whether the client's IP address is obtained from a DHCP server or is fixed. The registration occurs during the following events:

- When the client starts and the DHCP Client service is started.
- When an IP address is configured, added, or changed on any network connection.
- When an administrator runs ipconfig /registerdns.

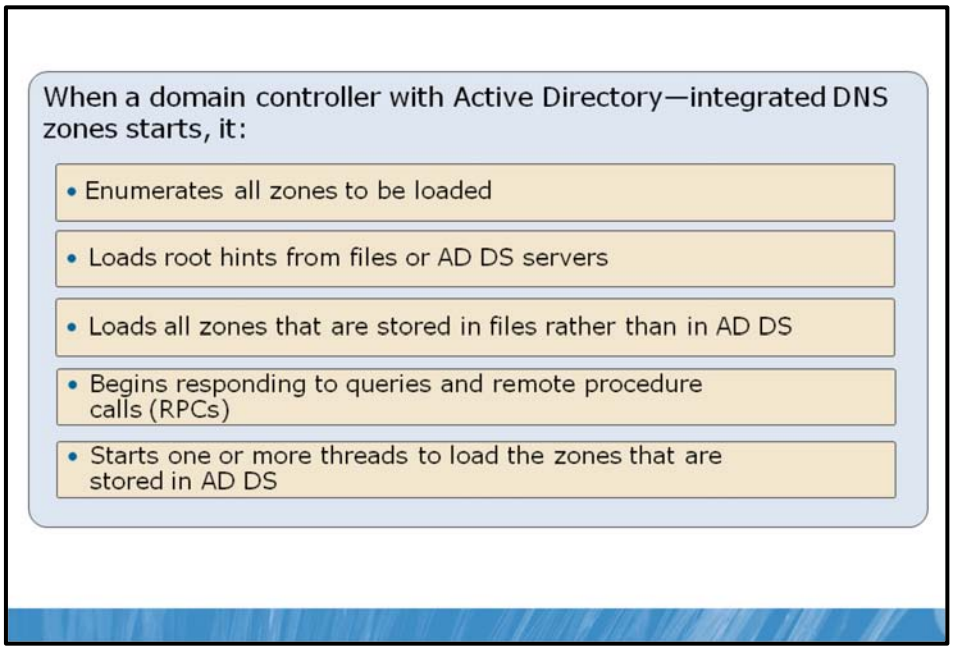
The client attempts to identify the DNS server that is the primary DNS server for the zone. If the zone is not an Active Directory–integrated zone, this may require several iterations in which the client identifies a name server, sends an update, and is refused because the name server hosts only a secondary zone. Eventually, if the zone supports dynamic updates, the client reaches a DNS server that can write to the zone. This is the primary server for a standard, file-based zone or any DC that is a name server for an Active Directory-integrated zone.

If the zone is configured for secure dynamic updates, the DNS server refuses the change. The client then authenticates and re-sends the update.

In some configurations, you may not want clients to update their records even in a dynamic update zone. Alternatively, you can configure the DHCP server to register the records on the clients' behalf. By default, a client registers its A (host/address) record, and the DHCP server registers the PTR (pointer/reverse lookup) record. PTR records are discussed in Lesson 4.

MCT USE ONLY. STUDENT USE PROHIBITED

Background Zone Loading

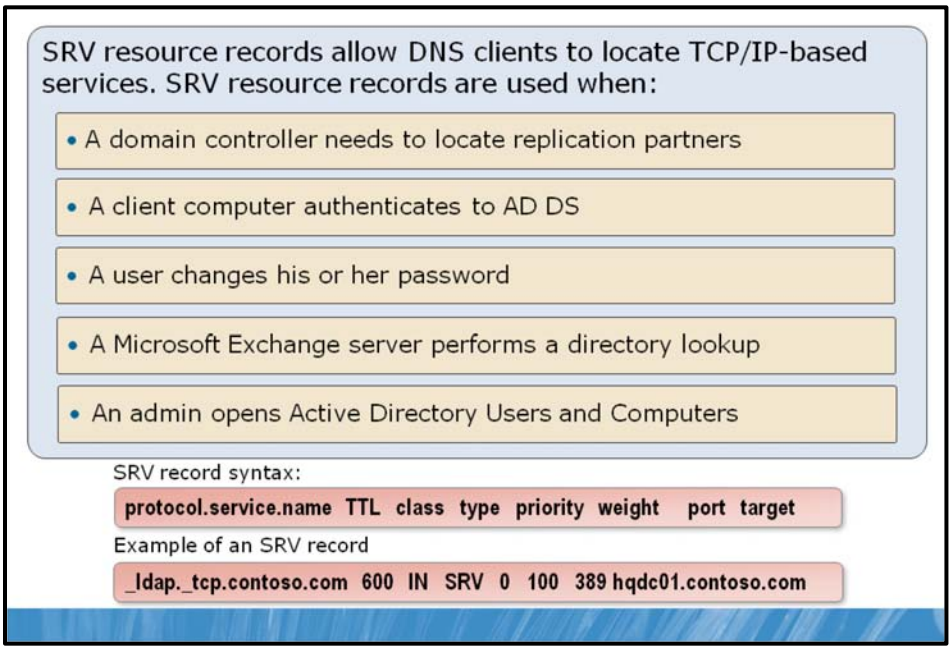

When a domain controller with Active Directory—integrated DNS zones starts, it:
• Enumerates all zones to be loaded
• Loads root hints from files or AD DS servers
• Loads all zones that are stored in files rather than in AD DS
• Begins responding to queries and remote procedure calls (RPCs)
• Starts one or more threads to load the zones that are stored in AD DS

It is possible for a zone that supports an AD DS domain to be quite large, particularly if the A records for clients are maintained in a large domain. In the previous versions of Windows, it took a long time for the DNS Server service to start when it had to load a large zone.

Windows Server 2008 loads zones in the background, allowing the DNS server to start responding to queries very quickly. If a query is sent for a zone that is not yet loaded, the server works to load that zone.

MCT USE ONLY. STUDENT USE PROHIBITED

Service Locator Records


SRV resource records allow DNS clients to locate TCP/IP-based services. SRV resource records are used when:
• A domain controller needs to locate replication partners
• A client computer authenticates to AD DS
• A user changes his or her password
• A Microsoft Exchange server performs a directory lookup
• An admin opens Active Directory Users and Computers
SRV record syntax:
protocol.service.name TTL class type priority weight port target
Example of an SRV record
_ldap._tcp.contoso.com 600 IN SRV 0 100 389 hqdc01.contoso.com

A Service Locator (SRV) resource record resolves a query for a network service, allowing a client to locate a host that provides a specific service.

SRV records are used in the following and many other scenarios:

- When a domain controller needs to replicate changes from its partners
- When a client computer needs to authenticate to AD DS
- When a user changes the password
- When an Microsoft Exchange server performs a directory lookup
- When an administrator opens Active Directory Users and Computers

An SRV record follows the syntax shown here.

```
protocol.service.name TTL class  type  priority weight port   target
```

An example of an SRV record is shown here.

```
_ldap._tcp.contoso.com  600 IN SRV   0   100   389 NYC-DC1.contoso.com
```

The components of the record are:

- The protocol service name, such as the LDAP service, offered by a domain controller.
- The time-to-live value, in seconds.
- The class (all records in a Windows DNS server will be IN or INternet).
- The type: SRV.
- The priority and weight, which help clients determine which host should be preferred.

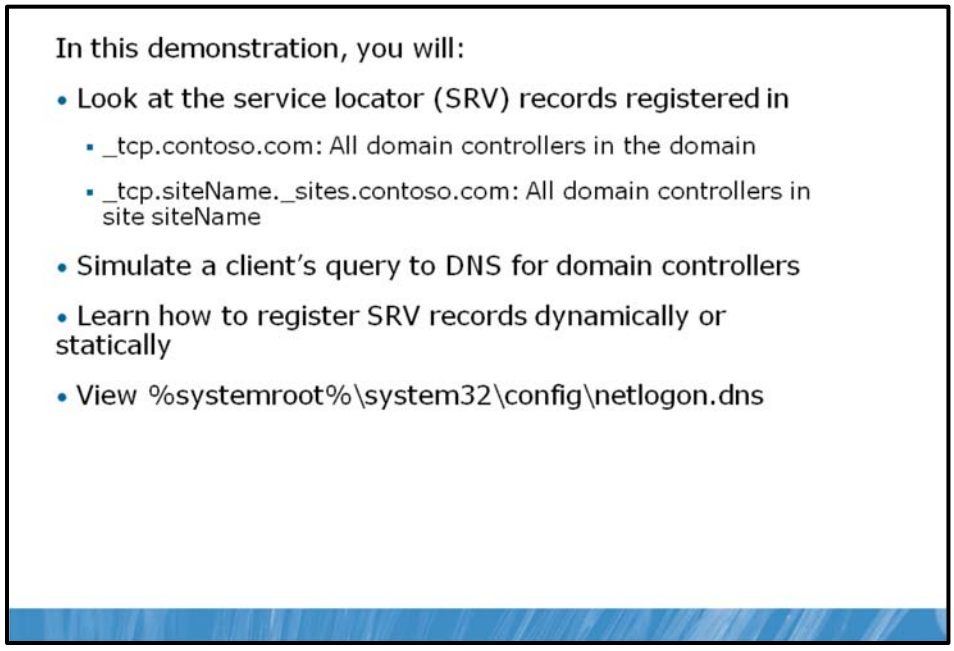
MCT USE ONLY. STUDENT USE PROHIBITED

- The port on which the service is offered by the server. Port 389 is the standard port for LDAP on a Windows DC.
- The target, or host of the service, which in this case is the domain controller named NYC-DC1.contoso.com.

When a client process looks for a domain controller, it can query DNS for an LDAP service. The query returns both the SRV record and the A record for the server(s) that provide the requested service.

MCT USE ONLY. STUDENT USE PROHIBITED

Demonstration: SRV Resource Records Registered by AD DS Domain Controllers


In this demonstration, you will:
• Look at the service locator (SRV) records registered in
▪ _tcp.contoso.com: All domain controllers in the domain
▪ _tcp.siteName._sites.contoso.com: All domain controllers in site siteName
• Simulate a client's query to DNS for domain controllers
• Learn how to register SRV records dynamically or statically
• View %systemroot%\system32\config\netlogon.dns

In this demonstration, you will see the SRV records registered by a domain controller in the contoso.com forest. You will:

- Use DNS Manager to see the service locator records registered in.
  - tcp.contoso.com, which lists all domain controllers in the domain
  - tcp.siteName._sites.contoso.com, which lists domain controllers that are covering a specific site
  - msdcs.contoso.com, which tracks the domain controllers in a forest and is used by DCs to locate each other
- Simulate a client query for a domain controller.

```
nslookup
set type=srv
_ldap._tcp.contoso.com
```

- Learn how domain controllers register their resource records in a dynamic update zone. Delete an SRV record, and then stop and restart the NetLogon service. The NetLogon service registers DC records at startup.
- View the %systemroot%\system32\config\netlogon.dns file, which contains the records that must be registered manually if the zone does not support dynamic updates.

Demonstration Steps

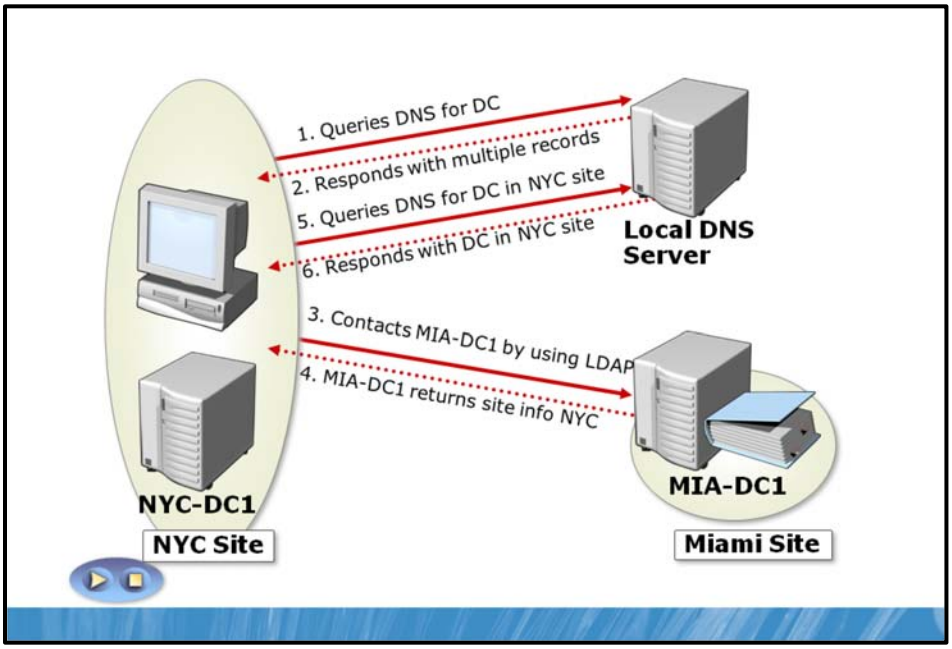
1. Run **DNS Management** with administrative credentials by using the account **Pat.Coleman_Admin** with the password **Pa$$w0rd**. Then, in the console tree, expand **NYC-DC1**, **Forward Lookup Zones,** and **contoso.com**, and then click the **_tcp** node. Examine the SRV records.

MCT USE ONLY. STUDENT USE PROHIBITED

2. In the console tree, expand **NYC-DC1**, **Forward Lookup Zones**, **contoso.com**, **_sites**, **Default-First-Site-Name**, and then click the **_tcp** node. Examine the SRV records.
3. Run **Command Prompt** with the administrative credentials used earlier.
4. Type **nslookup**, and then press Enter.
5. Type **set type=srv**, and then press Enter.
6. Type **_ldap._tcp.contoso.com,** and then press Enter.
7. Switch to **DNS Manager**.
8. Expand **NYC-DC1**, **Forward Lookup Zones,** and **contoso.com**, and then click the **_tcp** node.
9. Right-click the SRV records for **NYC-DC1.contoso.com**, and then click **Delete.**
10. Stop and start the netlogon service.
11. In the DNS console tree, right-click the **_tcp** node, and then click **Refresh**. Examine the SRV records for**NYC-DC1.contoso.com**.
12. Open **%systemroot%\system32\config\netlogon.dns** file in notepad
13. Examine the default SRV records.

MCT USE ONLY. STUDENT USE PROHIBITED

Domain Controller Location


1. Queries DNS for DC
2. Responds with multiple records
5. Queries DNS for DC in NYC site
6. Responds with DC in NYC site
Local DNS Server
3. Contacts MIA-DC1 by using LDAP
4. MIA-DC1 returns site info NYC
NYC-DC1
NYC Site
MIA-DC1
Miami Site

When a client authenticates, it attempts to locate a domain controller in its site. If a client has not authenticated before, it queries _ldap._tcp.domainName, and retrieves a list of all domain controllers in the domain. The client attempts an LDAP bind with each, and the first DC to respond is selected for the next step. Note that, at this point, it is possible that a domain controller in another site responds first.

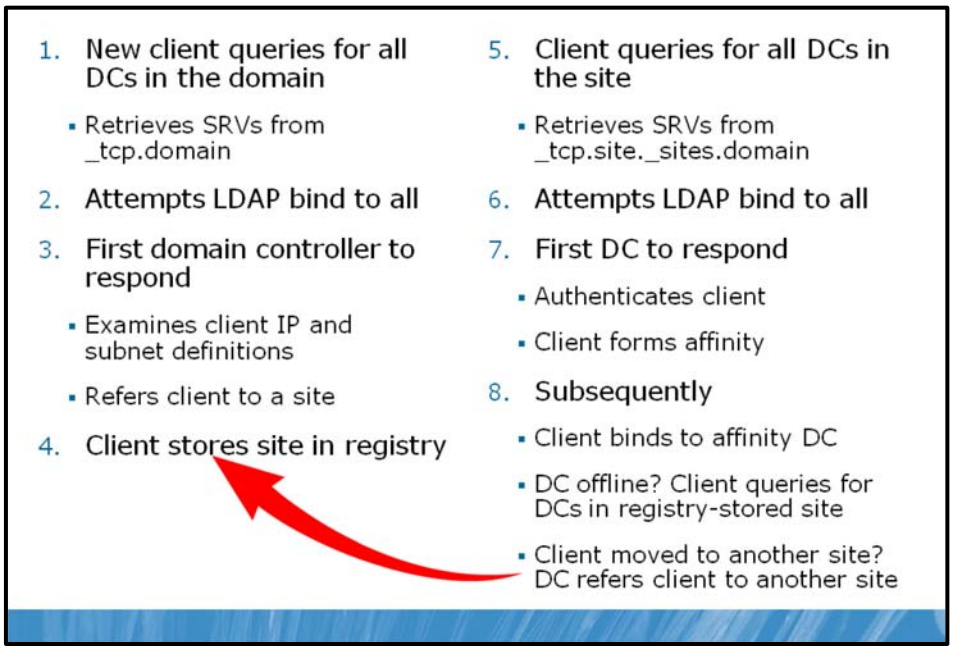
The client then attempts to authenticate with the domain controller. The domain controller examines the client's IP address and compares it with the information about sites and subnets. If the domain controller is not in the client's site, it tells the client what site the client is in.

The client then queries DNS for _ldap._tcp.siteName. domainName, which returns a list of domain controllers that are covering that site. Again, the client attempts an LDAP bind with each, and the first one to respond is selected. The client then proceeds to authenticate with that domain controller.

The client stores its site membership in the registry, and it forms an affinity with the domain controller with which it is authenticated. The next time the client needs to contact a domain controller, it starts with its affinity domain controller. If that domain controller is not available, the client retrieves its site information from the registry and queries for _ldap._tcp.siteName.domainName.

MCT USE ONLY. STUDENT USE PROHIBITED

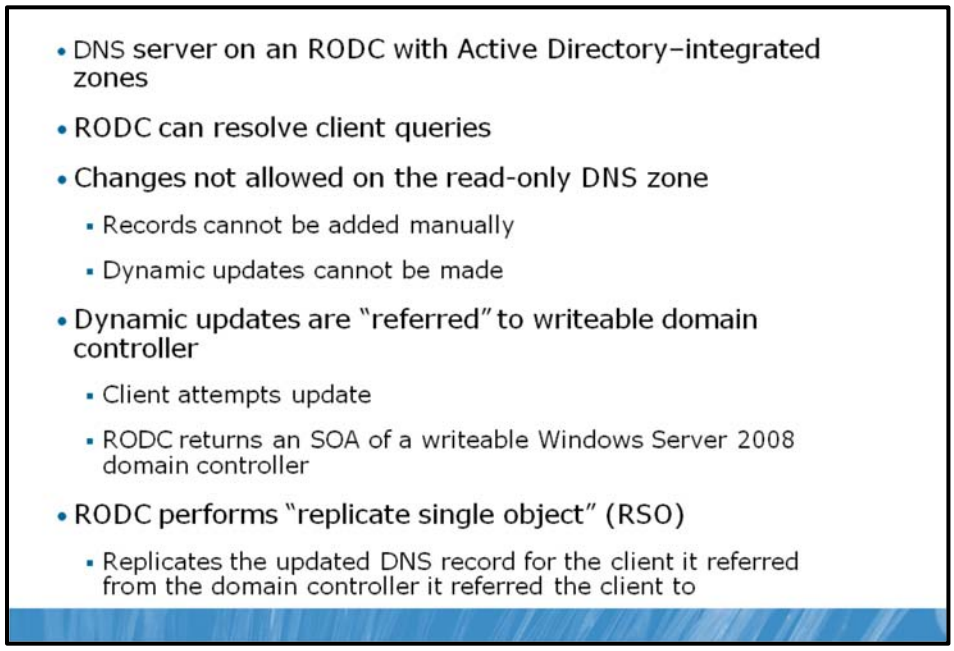
The process is summarized in the following slide:


1. New client queries for all DCs in the domain
▪ Retrieves SRVs from _tcp.domain
2. Attempts LDAP bind to all
3. First domain controller to respond
▪ Examines client IP and subnet definitions
▪ Refers client to a site
4. Client stores site in registry
5. Client queries for all DCs in the site
▪ Retrieves SRVs from _tcp.site._sites.domain
6. Attempts LDAP bind to all
7. First DC to respond
▪ Authenticates client
▪ Client forms affinity
8. Subsequently
▪ Client binds to affinity DC
▪ DC offline? Client queries for DCs in registry-stored site
▪ Client moved to another site? DC refers client to another site

Domain controller location will be revisited in Module 13, where you will learn how SRV records and the domain controller location process serve to localize authentication to an efficient domain controller.

MCT USE ONLY. STUDENT USE PROHIBITED

Read-Only DNS Zones


• DNS server on an RODC with Active Directory–integrated zones
• RODC can resolve client queries
• Changes not allowed on the read-only DNS zone
▪ Records cannot be added manually
▪ Dynamic updates cannot be made
• Dynamic updates are "referred" to writeable domain controller
▪ Client attempts update
▪ RODC returns an SOA of a writeable Windows Server 2008 domain controller
• RODC performs "replicate single object" (RSO)
▪ Replicates the updated DNS record for the client it referred from the domain controller it referred the client to

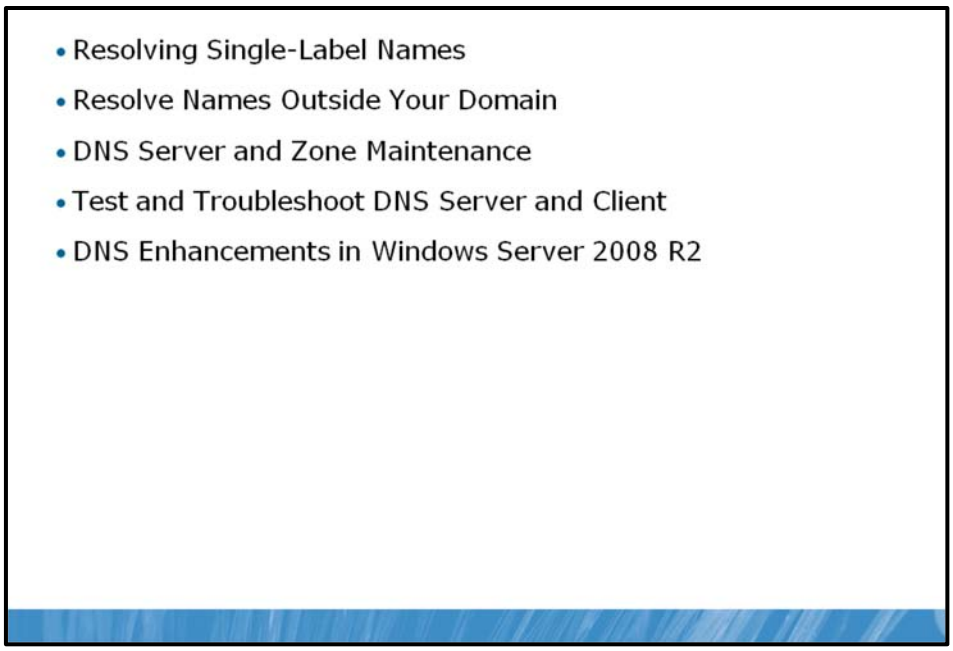
A DNS server on a Read-Only Domain Controller (RODC) can be authoritative for zones that are replicated to the RODC and can resolve queries for clients that use the RODC as their DNS server.

Of course, a key characteristic of an RODC is that it cannot make changes to Active Directory, so resource records cannot be added manually to the zone on an RODC, and dynamic updates are not accepted from clients.

Dynamic updates are serviced by referring clients to a writeable domain controller when they attempt to send an update to an RODC. It is useful for the RODC to include the client's updated resource record in the zone as quickly as possible, so the RODC tracks the client that attempted the update, and the writable domain controller to which the client was referred. After a short wait, the RODC performs a replicate single object (RSO) operation in which it retrieves the updated DNS record for the client from the writable domain controller, bypassing standard replication mechanisms.

MCT USE ONLY. STUDENT USE PROHIBITED

Lesson 3
Advanced DNS Configuration and Administration


• Resolving Single-Label Names
• Resolve Names Outside Your Domain
• DNS Server and Zone Maintenance
• Test and Troubleshoot DNS Server and Client
• DNS Enhancements in Windows Server 2008 R2

You've learned how to configure a simple DNS implementation and how DNS supports AD DS. In this module, you will explore selected topics of advanced DNS configuration and administration.

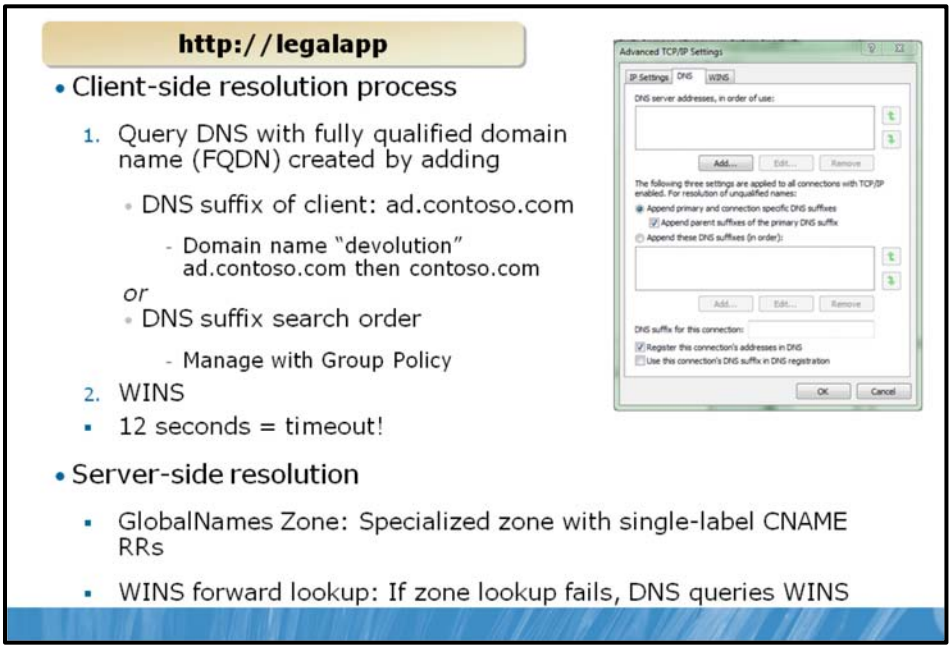
Objectives

After completing this lesson, you will be able to:

- Understand and configure single-label name resolution.
- Configure advanced DNS server settings.
- Audit, maintain, and troubleshoot the DNS server role.
- Describe DNS enhancements in Windows Server 2008 R2

MCT USE ONLY. STUDENT USE PROHIBITED

Resolving Single-Label Names


http://legalapp
• Client-side resolution process
1. Query DNS with fully qualified domain name (FQDN) created by adding
• DNS suffix of client: ad.contoso.com
- Domain name "devolution" ad.contoso.com then contoso.com
or
• DNS suffix search order
- Manage with Group Policy
2. WINS
▪ 12 seconds = timeout!
• Server-side resolution
▪ GlobalNames Zone: Specialized zone with single-label CNAME RRs
▪ WINS forward lookup: If zone lookup fails, DNS queries WINS

In the normal course of operations, a user or application may want or need to refer to a host by a single-label name. For example, a user may open Internet Explorer and browse to http://legalapp.

It is important that you understand how the DNS Client service works to resolve a single-label name.

First, the client tries to resolve the name as a fully qualified name by appending a DNS domain suffix to the single-label name. The suffix is determined by using one of the two following options, the first of which is configured in the Advanced TCP/IP Settings of a connection and the second by using Group Policy.

The DNS domain suffixes appended by the client are:

- The client's network connection DNS suffix. The client appends the suffix of its DNS connection, such as ad.contoso.com. If you can use the connection-based suffix, you can configure a client to use domain name devolution, which means that if the connection suffix fails, the client retries with the parent domain name, which would be contoso.com in this example. The devolution stops at that point—it does not query by using a top-level domain name.
- DNS suffix search order. You can specify the DNS suffixes that a client should try. This is easiest to manage by using Group Policy. If DNS suffix search order is used, there is no devolution. You must specify exactly the domain names you want the client to try.

If the DNS suffix does not result in a resolution, the DNS client gives up and queries DNS with a single-label name. If this does not work, NetBIOS name resolution is attempted, which starts with a query to a Windows Internet Name Service (WINS) server and, if that fails, resorts to a NetBIOS broadcast on the local segment.

The DNS client does not have much time in which to resolve the name. In fact, after 12 seconds, the resolution fails, at which point it is up to the client application to determine what steps to take. This means that it's possible that the client will time out before all name combinations are queried.

MCT USE ONLY. STUDENT USE PROHIBITED

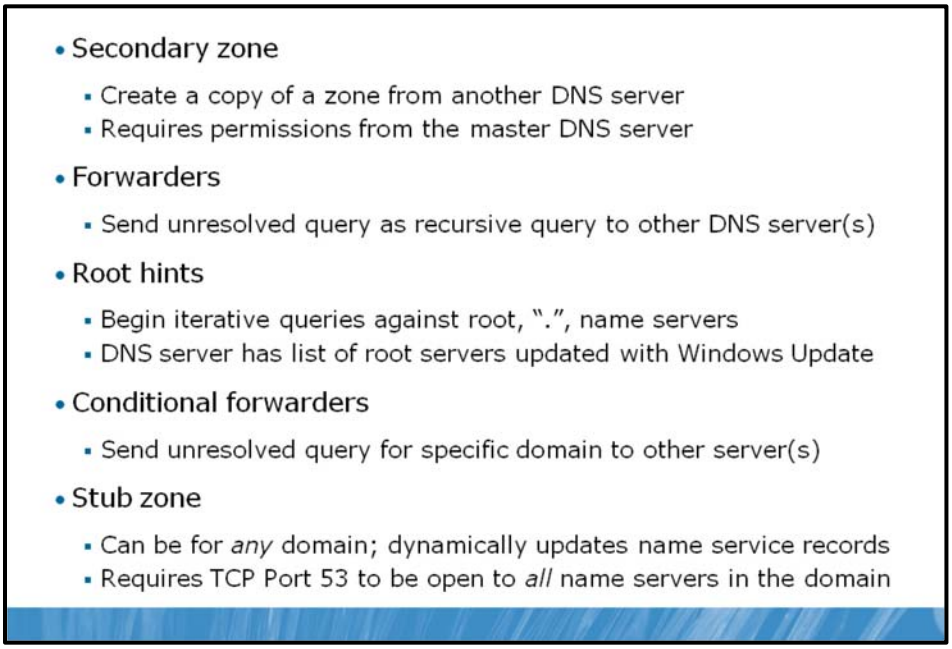
Windows Server 2008 DNS Server provides a new option to support the resolution of single-label names: the GlobalNames zone. The GlobalNames zone is a specialized zone that you create on your DNS servers. Typically, you would want it to be replicated in the ForestDNSZones partition so that it is available to all DNS servers in the forest. The zone contains CNAME records with a single-label names and their resolution to fully qualified domain names.

When a client submits a single-label query, the DNS server can resolve the query by retrieving the CNAME record from the GlobalNames zone and then looking up the appropriate A record for the FQDN.

To use GlobalNames, you must create the GlobalNames zone, and then enable its use in resolution by using the dnscmd.exe command. Details are available in the article listed under Additional Reading.

MCT USE ONLY. STUDENT USE PROHIBITED

Resolve Names Outside Your Domain

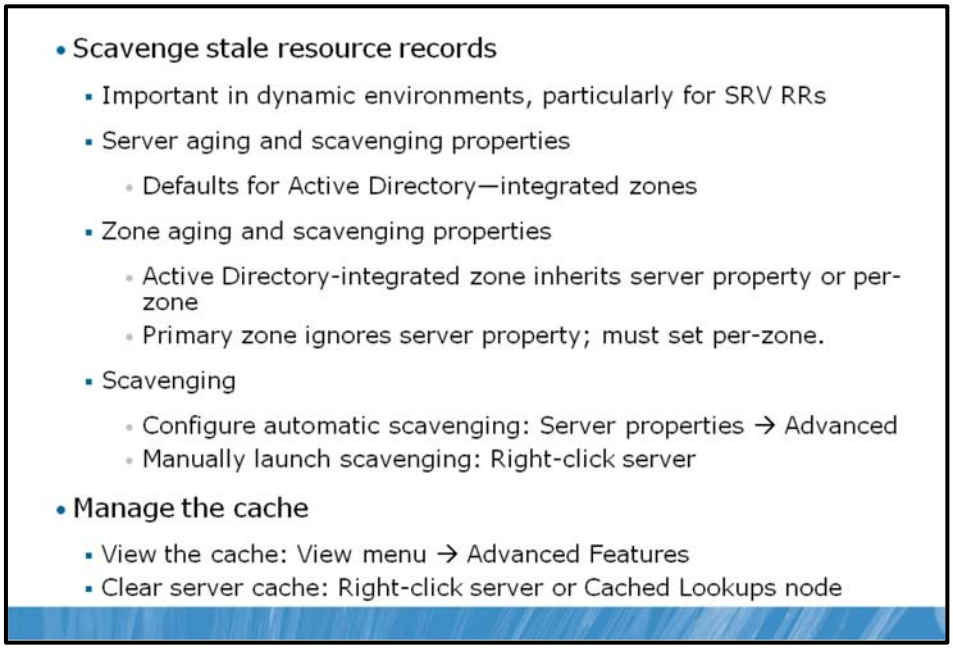

• Secondary zone
▪ Create a copy of a zone from another DNS server
▪ Requires permissions from the master DNS server
• Forwarders
▪ Send unresolved query as recursive query to other DNS server(s)
• Root hints
▪ Begin iterative queries against root, ".", name servers
▪ DNS server has list of root servers updated with Windows Update
• Conditional forwarders
▪ Send unresolved query for specific domain to other server(s)
• Stub zone
▪ Can be for *any* domain; dynamically updates name service records
▪ Requires TCP Port 53 to be open to *all* name servers in the domain

There are several ways to provide resolution for DNS records outside of your domain—records for which your DNS servers are not authoritative.

- Secondary zone. The first option is to make the servers authoritative by hosting a secondary zone of the external domain. This requires permission to perform a zone transfer from a name server in the zone, so it is typically not an option that is available for you to use for domains outside of your enterprise.
- Forwarders. Forwarders, detailed in Lesson 2, are pointers to upstream DNS servers, DNS servers provided by your ISP, or Internet DNS servers. Your DNS server can perform queries against servers listed as forwarders.
- If you choose to point to a DNS server other than one which you or your ISP maintain, it is best to ask permission before performing recursive queries against a third-party DNS server.
- Root hints. Root hints point to name servers for the root of the DNS namespace ("."). The DNS server has a list of root servers that is updated by Windows Update, though the list does not change often.
- Conditional forwarders. Conditional forwarders point to name servers against which to query for specific domain names. A conditional forwarder creates a direct shortcut to a server to query for a domain and bypasses the need to recursively query a (nonconditional) forwarder or to go to the root of the DNS namespace with a root hint.
- Stub zone. You learned about stub domains earlier in this module, because they can be used as a form of delegation for a child domain. Stub domains can also be very useful for resolving names outside your enterprise. Remember that the key benefit of a stub domain is that the DNS server dynamically maintains the list of name servers for the domain. You can think of a stub zone as a dynamic conditional forwarder. The "cost" is that TCP port 53 must be open to all name servers of the domain.

MCT USE ONLY. STUDENT USE PROHIBITED

DNS Server and Zone Maintenance


• Scavenge stale resource records
▪ Important in dynamic environments, particularly for SRV RRs
▪ Server aging and scavenging properties
◦ Defaults for Active Directory—integrated zones
▪ Zone aging and scavenging properties
◦ Active Directory-integrated zone inherits server property or per-zone
◦ Primary zone ignores server property; must set per-zone.
▪ Scavenging
◦ Configure automatic scavenging: Server properties → Advanced
◦ Manually launch scavenging: Right-click server
• Manage the cache
▪ View the cache: View menu → Advanced Features
▪ Clear server cache: Right-click server or Cached Lookups node

The DNS Server role is fairly self-maintaining; however, one feature is important to configure in a zone that supports dynamic updates: scavenging. Scavenging is the process of deleting aged records. It is important not only for client and server A records, but also for SRV records registered by domain controllers. In certain scenarios, it's possible to have SRV records that refer to incorrect, moved, or removed domain controllers. Scavenging ensures that they are eventually removed.

You can implement scavenging at the server or zone level for Active Directory-integrated zones. The server's Properties dialog box allows you to set server aging and scavenging properties, which act as the default for Active Directory-integrated zones, which inherit the server properties. You can override the server defaults on a zone-by-zone basis by using the zone's Properties dialog box.

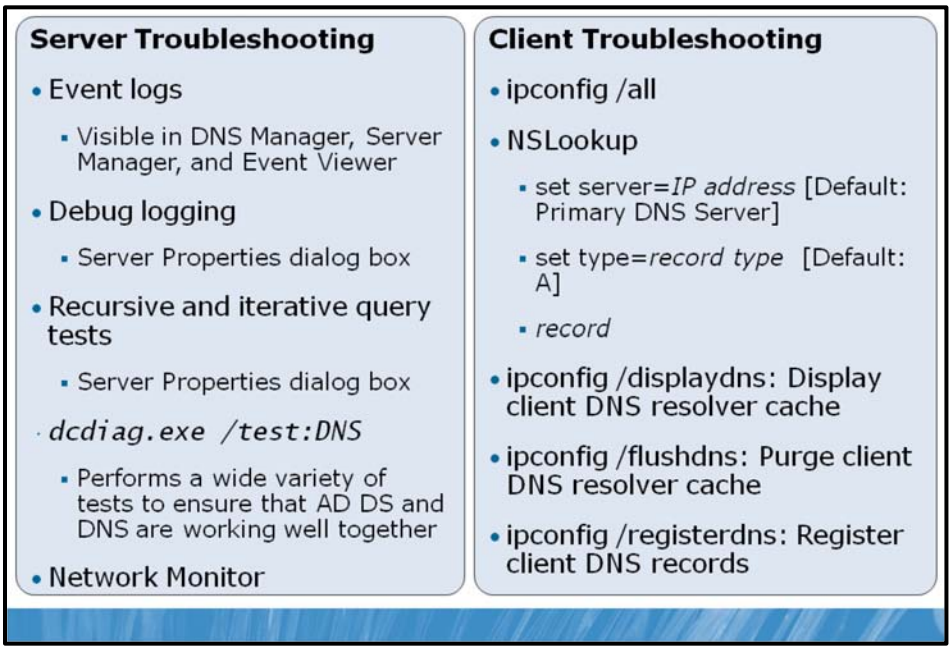
For standard primary zones, you must set scavenging at the zone level.

After you've specified the time limits after which scavenging of records is allowed, you must actually perform the scavenging. This is most easily managed by configuring the server for automatic scavenging, which can be done on the Advanced tab of the server's Properties dialog box. You can also manually initiate scavenging by right-clicking the server in the DNS Manager snap-in.

Another server maintenance task that you may need to perform is viewing or flushing the cache. This is useful when you discover that clients are obtaining incorrect resolutions from a server for zones for which it is not authoritative. You can view the Cached Lookups of a server by clicking the View menu in the DNS Manager snap-in and clicking Advanced Features. You can then clear the server cache, if necessary, by right-clicking the server node or the Cached Lookups node in the console tree.

MCT USE ONLY. STUDENT USE PROHIBITED

Test and Troubleshoot DNS Server and Client


Server Troubleshooting
• Event logs
▪ Visible in DNS Manager, Server Manager, and Event Viewer
• Debug logging
▪ Server Properties dialog box
• Recursive and iterative query tests
▪ Server Properties dialog box
dcdiag.exe /test:DNS
▪ Performs a wide variety of tests to ensure that AD DS and DNS are working well together
• Network Monitor
Client Troubleshooting
• ipconfig /all
• NSLookup
▪ set server=IP address [Default: Primary DNS Server]
▪ set type=record type [Default: A]
▪ record
• ipconfig /displaydns: Display client DNS resolver cache
• ipconfig /flushdns: Purge client DNS resolver cache
• ipconfig /registerdns: Register client DNS records

DNS events are logged in the DNS log, which is displayed in DNS Manager, Server Manager, and Event Manager. As with other event logs in Windows Server 2008, you can centralize the collection of events by using subscriptions, as detailed in Module 14. This is a recommended practice, because it allows you to keep an eye on a central location for signs of trouble in your DNS infrastructure.

Occasionally, it may be useful to perform debug logging, which logs details of DNS transactions. You can enable debug logging in the server's Properties dialog box.

Also in the server's Properties dialog box, you can perform test recursive and iterative queries to ensure that stub zones, conditional forwarders, forwarders, and root hints are working as expected.

The integration between DNS and AD DS was detailed in Lesson 2. The dcdiag.exe /test:DNS command performs an exhaustive series of tests to ensure that this integration is working. You can perform a more granular test if you suspect a specific problem. Type **dcdiag.exe /?** for more details.

DNS and the DNS Server role are all about resolving client queries. Sometimes, you need to troubleshoot the client-side experience and components of DNS.

You can use the following commands to troubleshoot the client side of DNS.

- **ipconfig /all.** This command displays the IP configuration of the client, including its DNS servers. Make sure that the client is using the correct servers, and that those servers are accessible.
- **NSLookup.** This performs DNS queries directly. A typical test with NSLookup includes:

```
set server=IP address
```

The preceding query specifies the DNS server to query. The default is the primary DNS server of the client. When a response is received, NSLookup identifies the server that returned the response. If a reverse lookup zone is not available with a PTR record containing the IP address of the DNS server, the DNS server's name will display as Unknown, but its IP address will be identified. The next line is:

MCT USE ONLY. STUDENT USE PROHIBITED

```
set type=record type
```

This line sets the type of record to query, such as SRV. The default is an address/host (A) record. The last line is:

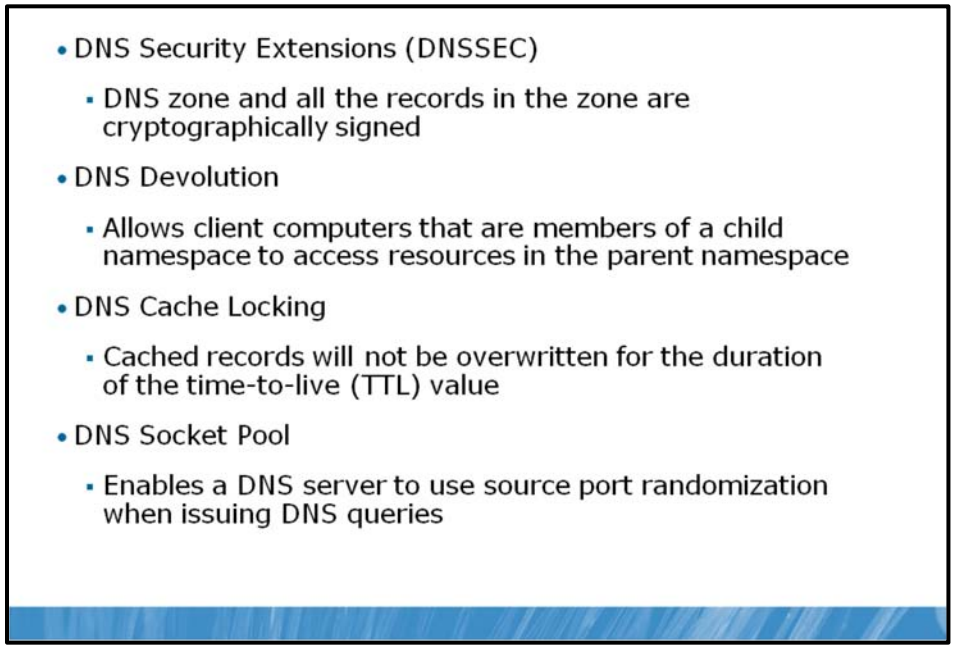
```
record
```

This specifies the record to query, which is typically a fully qualified domain name when the resolution of an A record is being tested.

- **ipconfig /displaydns.** This command shows the contents of the DNS resolver cache on the client.
- **ipconfig /flushdns.** This purges the client's DNS resolver cache.
- **ipconfig /registerdns.** This command triggers a dynamic update in which the client registers its A records.

MCT USE ONLY. STUDENT USE PROHIBITED

DNS Enhancements in Windows Server 2008 R2


• DNS Security Extensions (DNSSEC)
▪ DNS zone and all the records in the zone are cryptographically signed
• DNS Devolution
▪ Allows client computers that are members of a child namespace to access resources in the parent namespace
• DNS Cache Locking
▪ Cached records will not be overwritten for the duration of the time-to-live (TTL) value
• DNS Socket Pool
▪ Enables a DNS server to use source port randomization when issuing DNS queries

Windows Server 2008 R2 provides several enhancements to DNS. These enhancements provide additional security and functionality for this important service.

DNS Security Extensions

As DNS security threats become more topical, it is important to realize that securing the DNS is critical to securing enterprise networks and the Internet. DNS is often subject to man-in-the-middle, spoofing, and cache-poisoning attacks that are hard to defend against.

DNS Security Extensions (DNSSEC) allows for a DNS zone and all the records in the zone to be cryptographically signed. When a DNS server hosting a signed zone receives a query, it returns the digital signatures in addition to the records queried for. A resolver or another server can obtain the public key of the public/private key pair and validate that the responses are authentic and have not been tampered with. To do so, the resolver or server must be configured with a trust anchor for the signed zone, or for a parent of the signed zone.

The DNSSEC implementation in Windows Server 2008 R2 DNS server provides the ability to sign both file-backed and Active Directory–integrated zones through an offline zone signing tool. This signed zone will then replicate or zone transfer to other authoritative DNS servers. When configured with a trust anchor, a DNS server is capable of performing DNSSEC validation on responses received on behalf of the client.

The DNS client in Windows Server 2008 R2 and Windows 7 is a nonvalidating security-aware stub resolver. This means that the DNS client will offload the validation responsibilities to its local DNS server, but the client is capable of consuming DNSSEC responses. The DNS client's behavior is controlled by a policy that determines whether the client should check for validation results for names within a given namespace. The client will return the results of the query to the application only if validation has been successfully performed by the server.

MCT USE ONLY. STUDENT USE PROHIBITED

MCT USE ONLY. STUDENT USE PROHIBITED

DNS Devolution

Devolution is a behavior in Active Directory environments that allows client computers that are members of a child namespace to access resources in the parent namespace without the need to explicitly provide the fully qualified domain name (FQDN) of the resource.

With devolution, the DNS resolver creates new FQDNs by appending the single-label, unqualified domain name with the parent suffix of the primary DNS suffix name, and the parent of that suffix, and so on, stopping if the name is successfully resolved or at a level determined by devolution settings. Devolution works by removing the left-most label and continuing to get to the parent suffix.

For example, if the primary DNS suffix is central.contoso.com and devolution is enabled with a devolution level of two, an application attempting to query the host name emailsrv7 will attempt to resolve emailsrv7.central.contoso.com and emailsrv7.contoso.com. If the devolution level is three, an attempt will be made to resolve emailsrv7.central.contoso.com, but not emailsrv7.contoso.com.

The DNS client in Windows Server 2008 R2 and Windows 7 introduces the concept of a devolution level, which provides control of the label where devolution will terminate. Previously, the effective devolution level was two. An administrator can now specify the devolution level, allowing for precise control of the organizational boundary in an Active Directory domain when clients attempt to resolve resources within the domain. This update to DNS devolution is also available for previous versions of Microsoft Windows.

DNS Cache Locking

Cache locking is a new feature available if your DNS server is running Windows Server 2008 R2. When you enable cache locking, the DNS server will not allow cached records to be overwritten for the duration of the TTL value. Cache locking provides for enhanced security against cache poisoning attacks. You can also customize the settings used for cache locking.

When a recursive DNS server responds to a query, it will cache the results obtained so that it can respond quickly if it receives another query requesting the same information. The period of time the DNS server will keep information in its cache is determined by the TTL value for a resource record. Until the TTL period expires, information in the cache might be overwritten if updated information about that resource record is received. If an attacker successfully overwrites information in the cache, they might be able to redirect traffic on your network to a malicious site.

Cache locking is configured as a percent value. For example, if the cache locking value is set to 50, the DNS server will not overwrite a cached entry for half of the duration of the TTL. By default, the cache locking percent value is 100. This means that cached entries will not be overwritten for the entire duration of the TTL. The cache locking value is stored in the CacheLockingPercent registry key located in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\DNS\Parameters. If the registry key is not present, the DNS server will use the default cache locking value of 100.

DNS Socket Pool

The socket pool enables a DNS server to use source port randomization when issuing DNS queries. This provides enhanced security against cache poisoning attacks.

A DNS server running Windows Server 2008 R2 or a server that has installed security update MS08-037, will use source port randomization to protect against DNS cache poisoning attacks. With source port randomization, the DNS server will randomly pick a source port from a pool of available sockets that it opens when the service starts.

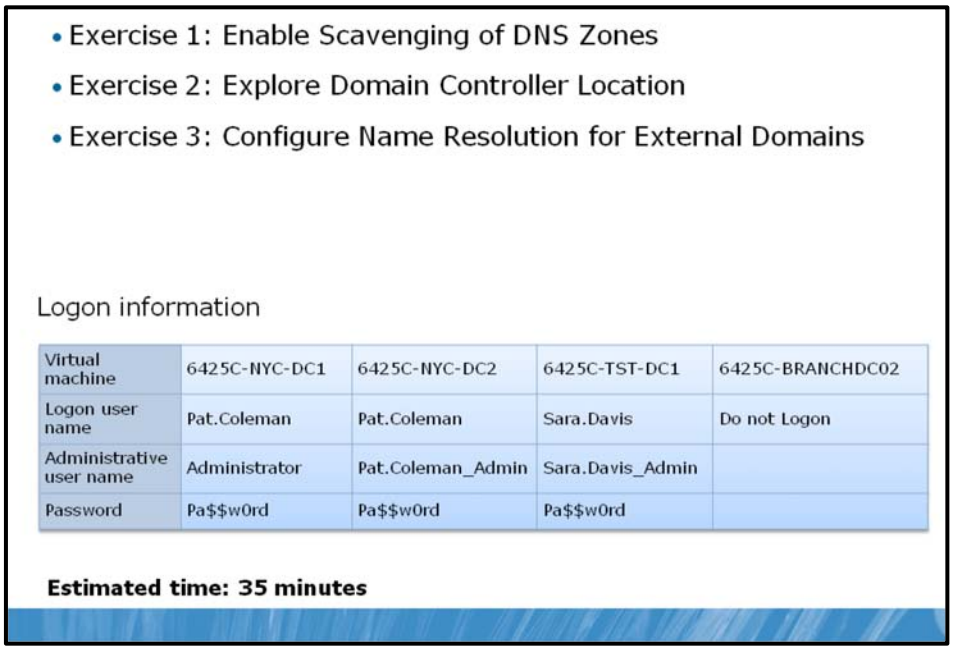
Instead of using a predicable source port when issuing queries, the DNS server uses a random port number selected from this pool, known as the socket pool. The socket pool makes cache poisoning

attacks more difficult because an attacker must correctly guess the source port of a DNS query in addition to a random transaction ID to successfully execute the attack.

The default size of the socket pool is 2,500. When you configure the socket pool, you can choose a size value from 0 to 10000. The larger the value, the greater protection you will have against DNS spoofing attacks. If you configure a socket pool size of zero, the DNS server will use a single socket for remote DNS queries. If the DNS server is running Windows Server 2008 R2, you can also configure a socket pool exclusion list.

MCT USE ONLY. STUDENT USE PROHIBITED

Lab B: Advanced Configuration of DNS



Some of the virtual machines should already be started and available after completing Lab A. However, if they are not, you should go through Exercises 1 and 2 in Lab A before continuing because there are dependencies between Lab A and Lab B.

1. On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Hyper-V Manager, click **6425C-NYC-DC1**, and in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Log on by using the following credentials:
   - User name: **Pat.Coleman**
   - Password: **Pa$$w0rd**
   - Domain: **Contoso**
5. Open Windows Explorer and then browse to **D:\Labfiles\Lab11b**.
6. Run **Lab11b_Setup.bat** with administrative credentials. Use the account **Administrator** with the password **Pa$$w0rd**.
7. The lab setup script runs. When it is complete, press any key to continue.
8. Close the Windows Explorer window, **Lab11b**.
9. Repeat steps 2 and 3 for **6425C-NYC-DC2.**
10. Log on by using the following credentials:
    - User name: **Pat.Coleman**
    - Password: **Pa$$w0rd**
    - Domain: **Contoso**

MCT USE ONLY. STUDENT USE PROHIBITED

11. Repeat steps 2 and 3 for **6425C-TST-DC1.**
12. Log on by using the following credentials:
    - User name: **Sara.Davis**
    - Password: **Pa$$w0rd**
13. Repeat steps 2 and 3 for **6425C-BRANCHDC02**. Do not log on to BRANCHDC02.

Lab Scenario

You are the DNS administrator at Contoso, Ltd. You want to improve the health and efficiency of your DNS infrastructure by enabling scavenging and creating a reverse lookup zone for the domain. You also want to examine the records that enable clients to locate domain controllers. Finally, you are asked to configure name resolution between contoso.com and the domain of a partner company, tailspintoys.com.

MCT USE ONLY. STUDENT USE PROHIBITED

Exercise 1: Enable Scavenging of DNS Zones

In this exercise, you will enable scavenging of DNS zones to remove stale resource records.

The main tasks for this exercise are as follows:

1. Enable scavenging of a DNS zone.
2. Configure default scavenging settings.

▶ Task 1: Enable scavenging of a DNS zone

1. On NYC-DC2, run DNS Manager as an administrator, with the user name **Pat.Coleman_Admin** and the password **Pa$$w0rd**.
2. Enable scavenging for the contoso.com zone. Accept the defaults for scavenging-related intervals.

▶ Task 2: Configure default scavenging settings

- Configure NYC-DC2 so that, by default, scavenging is enabled for all zones. Accept the defaults for scavenging-related intervals.

Results: In this exercise, you configured scavenging of the contoso.com domain and enabled scavenging as the default for all zones.

MCT USE ONLY. STUDENT USE PROHIBITED

Exercise 2: Explore aDomain Controller Location

In this exercise, you will examine the resource records that allow clients to locate domain controllers.

The main tasks for this exercise are as follows:

1. Explore _tcp.
2. Explore _tcp.brancha._sites.contoso.com.

▶ Task 1: Explore _tcp

- Examine the records in _tcp.contoso.com. What do the records represent?

▶ Task 2: Explore _tcp.brancha._sites.contoso.com

- Examine the records in _tcp.brancha._sites.contoso.com. What do the records represent?

Results: In this exercise, you examined the SRV records in the contoso.com domain.

MCT USE ONLY. STUDENT USE PROHIBITED

MCT USE ONLY. STUDENT USE PROHIBITED

Exercise 3: Configure Name Resolution for External Domains

In this exercise, you will configure name resolution between two completely separate domains.

The main tasks for this exercise are as follows:

1. Configure a stub zone.
2. Configure a conditional forwarder.
3. Validate name resolution for external domains.

▶ Task 1: Configure a stub zone

- On NYC-DC2, create a stub zone for tailspintoys.com that refers to the IPv4 address **10.0.0.31** as the master server.

▶ Task 2: Configure a conditional forwarder

1. On TST-DC1, run DNS Management as an administrator, with the user name **Sara.Davis_Admin** and the password **Pa$$w0rd**.
2. Create a conditional forwarder for contoso.com that forwards to the IPv4 address **10.0.0.10**.

▶ Task 3: Validate name resolution for external domains

1. On TST-DC1, open a command prompt and type **nslookup www.development.contoso.com**, and then press Enter. The command should return the address **10.0.0.24**.
2. Switch to DNS Manager and create a host (A) record for www.tailspintoys.com that resolves to **10.0.0.143**.
3. On NYC-DC2, open a command prompt and type **nslookup www.tailspintoys.com**, and then press Enter. The command should return the address **10.0.0.143**.

Results: In this exercise, you configured DNS name resolution between the contoso.com and tailspintoys.com domains.

▶ To prepare for the next module

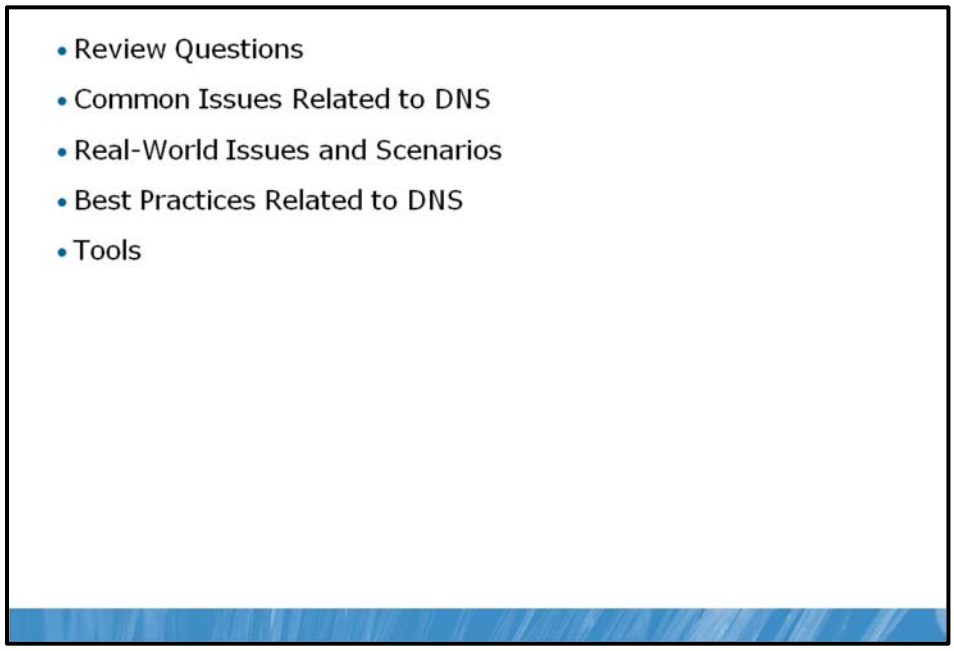
When you finish the lab, revert the virtual machines to their initial state. To do this, complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. Right-click **6425C-NYC-DC1**in the **Virtual Machines** list, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat these steps for 6425C-NYC-DC2, 6425C-TST-DC1, and 6425C-BRANCHDC02**.**

Lab Review Questions

Question: In this lab, you used a stub zone and a conditional forwarder to provide name resolution between two distinct domains. What other options you could have used?

Module Review and Takeaways



Review Questions

Question: You are conducting a presentation for a potential client about the advantages of using Windows Server 2008 R2. What are the new features that you would point out when discussing the Windows Server 2008 R2 DNS server role?

Question: You are deploying DNS servers into an Active Directory domain, and your customer requires that the infrastructure is resistant to single points of failure. What must you consider while planning the DNS configuration?

Question: You must automate a DNS server configuration process so that you can automate the deployment of Windows Server 2008. Which DNS tool can you use to do this?

Common Issues Related to DNS

Issue	Troubleshooting tip
Client can sometimes cache invalid DNS records	
Zone transfer is not working	

Real-World Issues and Scenarios

- DNS and Active Directory trusts

  When creating trusts between two Active Directory domains, the ability for domain A to lookup records in domain B (and vice versa) is tied to the configuration of the DNS infrastructure. Active Directory domains are accessible rarely on the Internet. Therefore, you need conditional forwarders, stub zones, or secondary zones to replicate the DNS infrastructure across domains and forests.

- Secure zones against zone dumping

MCT USE ONLY. STUDENT USE PROHIBITED

By default, zone transfers are disabled in Windows Server 2008. When configuring zone transfers, it is a best practice to specify the IP address of the servers to which you want to transfer zone data. Do not select the Allow zone transfer to Any Server, especially if the server is on the Internet. With this option enabled, it is possible to dump the entire zone, which can provide a significant amount of information about the network to possible attackers.

Best Practices Related to DNS

- If you are using Active Directory, use directory-integrated storage for your DNS zones. This offers increased security, fault tolerance, and simplified deployment and management.
- Disable recursion for servers that do not answer client queries or communicate by using forwarders. As DNS servers communicate amongst themselves by using iterative queries, this ensures that the server responds only to queries that are intended for it.
- Consider the use of secondary zones to assist in off-loading DNS query traffic wherever appropriate.
- Enter the correct email address of the responsible person for each zone you add to, or manage on, a DNS server. Applications use this field to notify DNS administrators for a variety of reasons. For example, query errors, incorrect data returned in a query, and security problems are a few ways in which this field can be used. Although most Internet email addresses contain the "@"symbol to represent the word "at" in email, this symbol must be replaced with a period (.) when entering an email address for this field. For example, instead of "administrator@microsoft.com," you would use "administrator.microsoft.com."

Tools

Tool	Used for	Where to find it
DNS Management Console	• DNS administration and management	Administrative Tools
Nslookup	• Use to perform query testing of the DNS domain namespace.	Command-line utility
Dnscmd	• Use this command-line interface to manage DNS servers. This utility is useful in scripting batch files to help automate routine DNS management tasks or to perform simple unattended setup and configuration of new DNS servers on your network.	Command-line utility
Ipconfig	• Use this command to view and modify IP configuration details that the computer uses. This utility includes additional command-line options to provide help in troubleshooting and supporting DNS clients.	Command-line utility
DNSlint	• Provides several automated tests to verify that DNS servers and resource records are configured properly and pointing to valid services. • You can download this command from Microsoft at http://go.microsoft.com/fwlink/?LinkID=214201	Command-line utility

MCT USE ONLY. STUDENT USE PROHIBITED

Windows Server 2008 R2 Features Introduced in This Module

Feature	Description
DNS Enhancements in Windows Server 2008 R2	New features in DNS that allow administrators to configure digital signing of DNS responses, cache locking, devolution and socket pooling.

MCT USE ONLY. STUDENT USE PROHIBITED

MCT USE ONLY. STUDENT USE PROHIBITED